UNIVERSIDADE FEDERAL DA INTEGRAÇÃO LATINO-AMERICANA, UNILA
INSTITUTO LATINO-AMERICANO DE ECONOMIA, SOCIEDADE E POLÍTICA, ILAESP
CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS E INTEGRAÇÃO

ESPIONAGEM E SOBERANIA NACIONAL: DILEMAS DE SEGURANÇA E DEFESA NO CASO BRASIL X EUA (2013)

ALEXANDRE DE OLIVEIRA MARTINS

Foz do Iguaçu 2014

UNIVERSIDADE FEDERAL DA INTEGRAÇÃO LATINO-AMERICANA, UNILA
INSTITUTO LATINO-AMERICANO DE ECONOMIA, SOCIEDADE E POLÍTICA, ILAESP
CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS E INTEGRAÇÃO

ESPIONAGEM E SOBERANIA NACIONAL: DILEMAS DE SEGURANÇA E DEFESA NO CASO BRASIL X EUA (2013)

ALEXANDRE DE OLIVEIRA MARTINS

Trabalho de Conclusão de Curso apresentado ao Instituto Latino-Americano de Economia, Sociedade e Política da Universidade Federal da Integração Latino-Americana, como requisito parcial à obtenção do título de Bacharel em Relações Internacionais e Integração.

Orientador: Prof. Dr. Lucas Kerr de Oliveira

Foz do Iguaçu 2014

ALEXANDRE DE OLIVEIRA MARTINS

ESPIONAGEM E SOBERANIA NACIONAL: DILEMAS DE SEGURANÇA E DEFESA NO CASO BRASIL X EUA (2013)

Trabalho de Conclusão de Curso apresentado ao Instituto Latino-Americano de Economia, Sociedade e Política da Universidade Federal da Integração Latino-Americana, como requisito parcial à obtenção do título de Bacharel em Relações Internacionais e Integração.

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. Lucas Kerr de Oliveira - UNILA

_____

Co-Orientadora: Profa. Dra. Tereza Maria Spyer Dulci - UNILA

_____

Prof. Mamadou Alpha Diallo - UNILA

_____

Prof. Marcelino Teixeira Lisboa - UNILA

Foz do Iguaçu, dezembro de 2014.

Dedico este trabalho à *Tríplice Fronteira*, prova viva de que todo rio tem sempre uma terceira margem.

AGRADECIMENTO

Agradeço ao professor e orientador Lucas Kerr, por socializar o que sua inteligência produz.
À professa Tereza Spyer, co-orientadora, pela assistência e incentivo.

A todos os professores da Unila, pela formação.

Aos colegas de curso, pela convivência.

À cidade e ao povo de Foz do Iguaçu, pela acolhida.

À educação pública, gratuita e de qualidade, sem a qual eu não acessaria o ensino superior.

Às políticas de assistência estudantil, que me permitiram dedicação integral aos estudos.

À minha família, pelo amor a distância.

A todos os amigos feitos em Foz, pela generosidade.

Não haverá império americano. O mundo é demasiado vasto, diverso e dinâmico para aceitar a predominância de uma única potência.

Emannuel Todd

MARTINS, Alexandre de Oliveira. **Espionagem e soberania nacional: dilemas de segurança e defesa no caso Brasil x EUA (2013)**. 2014. 86 páginas. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais e Integração) – Universidade Federal da Integração Latino-Americana, Foz do Iguaçu, 2014.

RESUMO

Este trabalho apresenta uma análise do chamado 'caso Snowden' e suas relações com a soberania brasileira. Ex-agente da inteligência norte-americana, Edward Snowden revelou ao jornalista Gleen Greenwlad, em junho de 2013, como funcionava o mais abrangente sistema espião até agora montado pela NSA, a agência nacional de inteligência estadunidense. A partir das cinco forças motrizes propostas por Buzan em seus Estudos de Segurança Internacional, o trabalho descreve, à luz da Escola de Copenhague, a política das grandes potência (focando na apresentação panorâmica da história dos EUA e na relação entre Estado e espionagem), os eventos históricos primordiais correlacionados ao tema, o desenvolvimento do aparato tecnológico e sua influência nas práticas de espionagem e nos serviços de inteligência, os debates acadêmicos e a institucionalização do tema no Brasil, finalizando com a discussão sobre a violação de soberania nacional.

Palavras-Chave: Espionagem, Edward Snowden, Estados Unidos, segurança e defesa, soberania, serviços de inteligência.

MARTINS, Alexandre de Oliveira. Espionaje y la soberanía nacional: los dilemas de seguridad y defensa en el Brasil vs EE.UU. (2013). 2014. 86 páginas. Trabajo de finalización de curso (graduación en Relaciones Internacionales e Integración) - Universidad Federal de la Integración Latinoamericana, Foz do Iguaçu, 2014.

RESUMEN

En este trabajo se presenta un análisis del llamado 'caso Snowden' y sus relaciones con la soberanía brasileña. Ex agente de la inteligencia de Estados Unidos, Edward Snowden reveló a lo periodista Glenn Greenwald, en junio de 2013, como funcionaba el más completo sistema de espionaje hasta el momento montado por la NSA, la agencia nacional de inteligencia de Estados Unidos. A partir de las cinco fuerzas motrices propuestas por Buzan en sus Estudios de Seguridad Internacional, el trabajo describe, a la luz de la Escuela de Copenhague, la política de las grandes potencias (centrando en la presentación panorámica de la historia de Estados Unidos y en la relación entre Estado y espionaje), los acontecimientos históricos primordiales relacionados con el tema, el desarrollo del aparato tecnológico y su influencia en las prácticas de espionaje y en los servicios de inteligencia, los debates académicos y la institucionalización del tema en Brasil, terminando con una discusión sobre la violación de la soberanía nacional.

Palabras clave: Espionaje, Edward Snowden, Estados Unidos, seguridad y defensa, soberanía, de inteligencia.

MARTINS, Alexandre de Oliveira. **Espionage and national sovereignty: dilemmas of security and defense in the Brazil vs. USA (2013)**. 2014. 86 pages. Conclusion Work Graduate (Degree in International Relations and Integration) - Federal University of Latin American Integration, Foz do Iguaçu, 2014.

ABSTRACT

This paper presents an analysis of so-called 'case Snowden' and its relationship with Brazilian sovereignty. Former agent of US intelligence, Edward Snowden revealed to journalist Glenn Greenwlad, in June 2013, how functioned the most comprehensive spy system so far mounted by the NSA, the National Agency of US intelligence. Based on five drives forces proposed by Buzan in his International Security Studies, the work describes, with help from the Copenhagen School, the policy of the great powers (focusing panoramic presentation of US history and the relationship between state and espionage); the primordial historical events related to the theme; the development of the technological apparatus and its influence on the practices of espionage (and on intelligence services); the academic debates and the institutionalization of the subject in Brazil; ending with a discussion on the violation of national sovereignty.

Keywords: Espionage, Edward Snowden, United States, security and defense, sovereignty, intelligence.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. PREÂMBULO, REFERENCIAIS TEÓRICOS E CATEGORIAS DE ANÁLISE

Cepik (2001) afirma que há dois usos principais do termo inteligência fora do âmbito das ciências cognitivas: uma definição ampla (de Jennifer Sims) diz que inteligência é toda informação coletada, organizada ou analisada para atender a demanda de um tomador de decisões – nesta acepção, inteligência é o mesmo que conhecimento ou informação; outra, mais restrita (de Abram Shulsky), diz que inteligência é a coleta de informações sem o consentimento, a cooperação ou mesmo o conhecimento por parte dos alvos da ação – nesta acepção, inteligência é o mesmo que segredo ou informação secreta. No âmbito deste trabalho, o termo *espionagem* será empregado como um processo de coleta *ilegal* de inteligência [podendo também em certos casos ser designado como 'atividades especiais' ou 'operações encobertas' por alguns autores e governos[1]] que deve ser distinguida da informação, sendo a inteligência, basicamente, a informação processada (Volkman, 2013). Em outras palavras, tratar-se-á a e*spionagem* como o 'como' se coleta *ilegalmente* uma informação, e *inteligência* como o sentido que se dá a tal informação. O Sistema Brasileiro de Inteligência (2004) considera inteligência

> "(...) como o exercício permanente de ações especializadas orientadas para obtenção de dados, produção e difusão de conhecimentos, com vistas ao assessoramento de autoridades governamentais, nos respectivos níveis e áreas de atribuição, para o planejamento, a execução e o acompanhamento das políticas de Estado, englobando também a salvaguarda de dados, conhecimentos, áreas, pessoas e meios de interesse da sociedade e do Estado". (SBI, 2004).

[1] Na verdade, operações encobertas são ferramentas de implementação de política, tais como sanções econômicas, ameaças de uso ou uso da força militar. São atividades governamentais voltadas para influenciar as condições políticas, econômicas ou militares no estrangeiro. Essa definição abarca um amplo leque de atividades situadas na zona cinzenta entre a diplomacia e a guerra: ações que vão do suporte relativamente 'aberto' a governos e forças políticas aliadas, até o uso de agentes de influência, agitação e propaganda, campanhas de desinformação, treinamento de guerrilhas, desestabilização de adversários, assassinatos, apoio a golpes de estado e operações paramilitares. A ênfase é posta na negação da autoria, mais do que na clandestinidade da operação em si mesmo. (Cepik, 2001)

Embora nessa definição *obtenção* e *processamento* estejam juntos, neste trabalho partiremos do pressuposto de que os recursos mobilizados para uma e para outro são sobremaneira distintos: a obtenção pressupõe um caráter mais ativo, interventor, enquanto o processamento um caráter mais passivo, acessório. Assim, apesar de 'monitoramento', 'vigilância' e 'espionagem' serem muitas vezes outros nomes que podem receber os Serviços de Inteligência, no contexto deste trabalho faremos uma distinção entre a obtenção *ilegal* de dados, que consideraremos *espionagem* e o processo que envolve a coleta (legal), a análise, a produção e o uso de dados, que chamaremos de *Inteligência*. A prática de uma ou de outra dependerá da relação que existirá entre os produtores da informação processada e seus usuários. Nesse sentido, como defende Afonso (2006), profissionalizar cada vez mais a Inteligência é uma necessidade que se impõe a cada dia, pois esse esforço passa pela perfeita visualização do ofício do profissional da área, cujas funções vão além da manufatura de relatórios e abrangem desde a sensibilização dos usuários para as questões de Inteligência até o estudo das patologias institucionais derivadas de sua própria existência, com o objetivo de elaborar e aperfeiçoar contrapesos e controles externos da atividade.

É fundamental, para Afonso (2006), que a Inteligência tome consciência completa de si para que possa educar e se impor de maneira benéfica, ocupando um lugar exclusivamente seu [e não da espionagem], pois, por mais que os serviços de inteligência sejam conscientes, falhas ocasionalmente ocorrerão, devido à má administração da interação entre produtores e usuários, principalmente aquelas falhas derivadas do aspecto da proximidade e da distância entre os dois atores. Nesse sentido, como expõe Cepik (2001), o *ethos* profissional da atividade de análise em inteligência e suas regras de produção de conhecimento são as mesmas que governam outra atividade de pesquisa, assim, também como em qualquer outra atividade desse tipo, os serviços de inteligência podem cair bem abaixo dos padrões esperados de isenção, relevância e qualidade das análises produzidas. Por isso mesmo, Afonso (2006) defende que em lugar nenhum no mundo se alcançou um modelo perfeito de inserção da Inteligência no processo decisório que a previna totalmente contra os vícios apresentados (espionagem, por exemplo). Entretanto, para Afonso (2006), os aparatos de Inteligência atuais são relativamente eficientes na identificação e reversão das mazelas e suas causas, incentivando o aprimoramento da discussão em torno desse tema e colocando ideias em prática, entretanto seria necessário, defende Afonso (2006), que profissionais de Inteligência e governantes conscientizados, em conjunto, desenvolvam continuamente meios cada vez mais capazes de minimizar as patologias que surjam da inexorável relação entre produtor e usuário, bem como nunca baseiem suas relações em axiomas e práticas sem alicerce teórico, mas em conceitos bem fundamentados e oxigenados pelo debate.

Buscando uma localização mais precisa da *espionagem* no campo dos saberes humanos, uma questão emerge: dado seu caráter acessório no processo decisório do Estado, em que área incluí-la? Embora variando, conforme o foco que se queira dar, social, psicológico, antropológico, bélico ou de segurança, a palavra 'espionagem', mesmo tendo tido seu significado alterado ao longo do tempo, mantém relações com suas origens etimológicas. Vinda da raiz latina "specere", metamorfoseou-se em "espionnage", no francês; em "spione", no italiano clássico; em "espier", no anglo-normando; e fornece o radical "spy", cuja presença em várias palavras antigas sempre significou "olhar e observar". Mas 'olhar e observar' de uma determinada forma, sigilosa, sem o conhecimento do sujeito/objeto observado; um 'olhar e observar' de um sujeito/objeto específico: aquele/aquilo que guarda interesses reais, pragmáticos e estratégicos ao observador; um 'olhar e observar' com fins bem claros de antever, de conhecer antes as possíveis ações do outro, mormente um inimigo, para que o observador possa reagir com precessão, evitando ser prejudicado pela ação a ser cogitada, a princípio em segredo, pelo outro; um 'olhar e observar' de causas múltiplas, variando segundo a natureza humana, segundo interesses materiais ou abstratos, em nome do egoísmo e até mesmo do coletivismo. Tendo, portanto, esse sentido mais profundo de preservação, a *espionagem* acaba por se inserir no escopo dos estudos de segurança (sensação) e defesa (ação)[2], já que, em última instância, as motivações maiores do ato de espionar é uma preocupação estratégica com a própria proteção ou a tentativa de dissuadir outrem de nos direcionar ações nocivas (pessoas ou Estados).

As origens da prática da espionagem remontam ao mundo antigo. Volkman (2013) pondera que desde que os seres humanos passaram a guerrear uns contra os outros, a espionagem é vital, pois envolve perguntas fundamentais como 'o que os inimigos potenciais estão planejando fazer? quais suas habilidades? quais são os perigos? quão iminentes são esses perigos?'. Segundo Volkman (2013), ninguém sabe ao certo e com exatidão quando a espionagem, como a conhecemos, começou, mas evidências arqueológicas antigas, do início da civilização, contêm traços de espionagem primitiva. Tabuletas de barro descobertas, gravadas mais de 4.000 anos atrás, mencionam operações de espionagem; entre elas, uma tabuleta

[2] Para Buzan et al. (1998), como não é possível medir a segurança objetivamente, uma abordagem objetivista da segurança só é viável em casos de ameaças inequívocas e imediatas, como tanques hostis cruzando a fronteira de um país. Mesmo nesse caso, no entanto, os autores observam que a condição de "hostilidade" resulta de uma relação constituída socialmente e, por conseguinte, não é objetiva; os tanques poderiam ser, por exemplo, parte de uma operação de paz. Para que uma questão seja considerada como de segurança, é necessário que isso seja estabelecido socialmente por meio de práticas intersubjetivas. Por isso consideramos a ESPIONAGEM como uma questão de segurança e defesa.

suméria descreve uma operação de espionagem que usava sinais de fogueiras acesas por espiões que trabalhavam dentro da cidade de Babilônia, para transmitir informações sobre as defesas da cidade. A mais antiga evidência detalhada de espionagem viria dos artefatos que se conservaram de uma das primeiras poderosas civilizações, a Assíria.

No século IV a.C., Sun Tzu, em "A arte da guerra", defendia que um líder vencedor seria aquele que baseasse sua razão na presciência, que não adviria de espíritos ou deuses, nem da analogia com ocorrências passadas ou de cálculo, mas, sim, por meio de homens espiões que conhecessem a situação do adversário. Ao longo da história, a ciência e a tecnologia proporcionaram ao homem um arsenal de instrumentos que permitiram inovar por diversas vezes os meios e métodos utilizados no período de Sun Tzu para obter informações. No decorrer do processo histórico, a atividade de espionagem foi promovida, principalmente, pelos Estados, com o objetivo de obter informações políticas ou militares e utilizá-las na formulação de estratégias de defesa ou ataque. Assim ocorreu na Primeira e na Segunda Guerras Mundiais e, especialmente, durante a Guerra Fria.

Volkman (2013) cita inúmeros casos de prática de espionagem, chamando a atenção: o dos gregos, que separavam o olheiro (geralmente soldado) e o espião (civil que vivia disfarçado em território inimigo); o dos romanos, cujo método preferido era o suborno e generosos pagamentos a chefes tribais aliados de Roma; o dos israelitas e o papel de Moisés e Josué, como estrategistas; o dos mongóis e o sistema de espionagem em dois níveis de Genghis Khan; o dos venezianos e o papel decisivo de Marco Polo; o de Sir Francis Walsingham, e sua percepção de que o que levava os homens a confiar era o que os movia a fazer o que faziam; o dos franceses, sob a liderança de Luís XIV e Armand Jean Duplessis (Cardeal Richelieu); o de Cromwell e seu homem de confiança Thurloe; o de Napoleão Bonaparte; o de Benjamin Franklin; o desenvolvido pela União e pela Confederação durante a Guerra de Secessão nos EUA; o do império austro-húngaro; o de T.E. Lawrence, o famoso "Lawrence da Arábia", que executou plano para ajudar na revolta árabe; o do nazismo; o da KGB; o do Vietnã; o da Mossad; o da CIA; o do MI6; o da NSA, entre outros. Volkman (2013) não cita, entretanto, o famoso caso cubano descrito por Pillas (1996), em que o governo dos EUA gastou milhões de dólares para montar e manter em funcionamento uma rede de espiões em Cuba, como parte das atividades destinadas a derrubar o regime de Fidel Castro, mas, em 1987, o governo cubano anunciou que havia controlado e filmado todas as operações clandestinas, que incluíam tentativas de sabotagem e de assassinato de Fidel, e a CIA descobriu que durante décadas havia sustentado agentes duplos. O exemplo cubano esteja talvez mais em harmonia com o que Keegan (2006) defende: na guerra, a inteligência, por melhor que seja, não é um guia infalível para a vitória,

que seria um prêmio fugidio, obtido mais com sangue do que com cérebros (mais com ideologia do que com cérebros, no caso cubano).

Para Volkman (2013), a inteligência funcionaria tradicionalmente em três níveis: estratégico (capacidades e intenções); tático (inteligência operacional) e contra-inteligência (proteção dos segredos de uma nação a partir de operações de espionagem de outras nações). Cepik (2002/2003) pleiteia que as categorias mais utilizadas convencionalmente ainda são disciplinares, dividindo os produtos da inteligência em, por exemplo, inteligência política (*como os militares russos reagirão à expansão da OTAN para o leste europeu?*), militar (*como funcionam os sistemas de aquisição de alvo das novas armas anti-balísticas norte-americanas em desenvolvimento?*), científica e tecnológica (*quais as prioridades atuais de pesquisa em sistemas óticos e lasers direcionais nos dez principais laboratórios europeus?*), econômica (*quais as consequências da reestruturação do sistema bancário japonês para as decisões de investimento dos países do leste asiático?*) e mesmo sociológica (*como a composição demográfica e religiosa do Cáucaso norte condiciona as chances do fundamentalismo wahabbita expandir-se no flanco sul da Rússia?*).

Do ponto de vista dos alvos das operações de inteligência, eles costumam ser divididos em transnacionais (terrorismo, crime organizado etc), regionais (África Austral, União Europeia etc), nacionais (EUA, China etc) e subnacionais (grupos militantes armados, máfias criminosas). Cepik (2001) recorda ainda que os serviços de inteligência modernos surgiram no contexto dos Estados absolutistas europeus, que procuravam generalizar a necessidade de reduzir custos na obtenção de informações e desejavam ampliar sua capacidade de dominação (*enforcement*). Buzan (2012) lembra que os territórios dos Estados eram valorizados por sua importância geopolítica e estratégica, além das capacidades materiais e econômicas que geravam, enquanto se dava pouca atenção às identidades e alianças dos povos que habitavam esses territórios, mas que o advento do nacionalismo mudou isso, já que com a afirmação de que as nações possuíam identidades específicas e que deveriam governar os territórios nos quais elas viviam, o nacionalismo sacralizou o território, especialmente por meio da soberania. Tal fenômeno acentuou a importância e necessidade de espionar o que o outro Estado fazia, sob a justificativa patriótica, nacionalista e estatal.

Como se pode deduzir, a prática de espionar, embora antiga e presente onde houvesse conflito e divergência entre seres humanos, tornou-se, então, quase um costume especialmente quando surge o Estado moderno e é comumente justificada em nome das razões de Estado maquiavélicas. E por que razão os Estados espionariam? Ao que parece, sobretudo quando os serviços de inteligência são insuficientes (atividades regulares) é que os Estados espionam

(agem irregularmente). Para Cepik (2001), as utilidades esperadas com a atividade regular de inteligência formam uma lista diversificada: 1) contribuir para tornar o processo decisório governamental nas áreas relevantes de envolvimento mais racional e realista; 2) fazer com que o processo interativo entre *policymakers* e oficiais de inteligência produza efeitos cumulativos de médio prazo aumentando o nível de especialização dos tomadores de decisões e de suas organizações; 3) apoiar diretamente o planejamento de capacidades defensivas e o desenvolvimento e/ou aquisição de sistemas de armas, de acordo com o monitoramento das sucessivas inovações e dinâmicas tecnológicas dos adversários; 4) apoiar mais diretamente as negociações diplomáticas em várias áreas, não tanto afetando a definição da política externa mas propiciando ajustes táticos derivados da obtenção de informações relevantes; 5) ser capaz de subsidiar o planejamento militar e a elaboração de planos de guerra, bem como suportar as operações militares de combate e outras (operações de paz, assistência, missões técnicas etc); 6) alertar os responsáveis civis e militares contra ataques surpresa, surpresas diplomáticas e graves crises políticas internas que podem nunca ocorrer, mas para as quais os governantes preferem 'assegurar-se' ao invés de arriscar; 7) monitorar os alvos e ambientes prioritários para reduzir incertezas e aumentar o conhecimento e a confiança, especialmente no caso de implementação de tratados e acordos internacionais sem mecanismos de isenção in loco; 8) servir para preservar o segredo sobre as necessidades informacionais, as fontes, fluxos, métodos e técnicas de inteligência diante da existência de adversários interessados em saber tais coisas.

Para cumprir tais objetivos regulares, os Estados muitas vezes cometem ações clandestinas e ilegais, assim, entre muitos motivos, espionariam para ter informações privilegiadas com antecedência. Espionariam por inúmeros interesses, mas todos relacionados à manutenção da existência do próprio Estado espião. A espionagem, entretanto, quando descoberta, traz à superfície uma prática do subterrâneo das relações internacionais, sabida pelos atores, mas só aceita em nome da implícita concorrência que os mesmos também indiretamente pactuam, de modo que, quando a espionagem é exposta, passa a constituir exatamente o momento em que a vitória de um Estado (o que descobriu) se dá sobre o outro (o que espionava). Na Guerra Fria, por exemplo, essa vitória fatalmente significava a liquidação do espião flagrado, quando não tornava mais tensa ainda a própria relação dos países envolvidos. Também durante este período, as técnicas e tecnologias tiveram um desenvolvimento tal que a captura do adversário, por escorregadia e de difícil comprovação que fosse, tinha de constantemente ser adiada, o que protelava os exercícios da espionagem e mantinha as aparências de normalidade na relação entre os Estados submetidos e comprometidos que estavam mutuamente com os ilícitos, licitamente aceitos se e somente se

em segredo.

Os espiões, homens de carne e osso, como bem ilustram desde agentes reais da KGB e da CIA à época da Guerra Fria, mas que compõem a estrutura estatal de quase todas as nações atuais, até fictícios, como o conhecido britânico James Bond, tinham seu ofício como profissão de fé e juravam fidelidade à pátria – à exceção de espiões mercenários, que, muitas vezes, vinculavam-se aos dois lados em contenda -, de modo que, a exemplo de representantes oficiais, uma vez recebida do país uma plenipotência para agir fossem por quais meios – legítimos ou não –, desde que em nome dos interesses daquilo que era sua própria razão de existir: seu país, sua nação, o Estado - assim o faziam em sua plenitude. Nesse sentido, traições, embora não raras, eram entendidas como fatalidades merecedoras de punições exemplares, já que representavam exceções a uma dura regra e que podiam colocar todo o jogo de espionagem em risco. Por isso é que ainda que tenham se sabido de vários casos clássicos de traições de ambos os lados na Guerra Fria, por exemplo, o caso do casal Julius e Ethel Rosenberg, dos EUA[3], ainda continuam sendo exceção a uma regra rigorosamente policiada pelos Estados por meio de suas complexas estruturas de Inteligência e Contra-inteligência, o que é compreensível se considerarmos que, como uma das condições da existência dessa prática é não ser descoberto, os verdadeiros ases da espionagem são aqueles que permanecem no anonimato e, portanto, de quem nunca toma-se conhecimento. O pós-Guerra Fria, em certa medida, desmistificou e destituiu o poder glamoroso de que gozavam os espiões, mas não os extinguiu.

O desenvolvimento da técnica de espionagem ocorreu em proporção direta ao aceleramento das tecnologias de informação e comunicação (TICs), que, por um lado, subtraíram do espião muitas funções antes necessariamente garantidas ‘in loco’; por outro lado, fizeram ascender um outro tipo de perfil humano espião, agora especializado em dominar programas, códigos e operações virtuais, sem necessariamente ter de fazer largos e perigosos deslocamentos geográficos. Esse ‘novo’ espião, embora também treinado em técnicas convencionais, o que não lhe tirou seu grau de profissão de risco, especializou-se, no entanto, em conhecimentos cibernéticos, línguas e técnicas modernas de suborno. As duas ‘qualidades’ lhe garantem o ofício: pessoalmente, é capaz de transmutar-se e dissimular para assegurar o sucesso de um engodo (como no caso da operação Argo, no Irã) ou, quando por si mesmo não obtém o que quer, tem os meios necessários para subornar ou comprar quem quer que seja;

[3] A versão oficial é a de que o casal teria entregado à União Soviética segredos militares obtidos por Julius, que trabalhava no exército dos EUA. Ambos foram presos em 1950 e, três anos depois, acabaram executados na cadeira elétrica. O irmão de Ethel, funcionário do Projeto Manhattan, que construiu a primeira bomba atômica, forneceu ao casal informações sobre armas nucleares. Os relatórios acabaram nas mãos dos soviéticos.

virtualmente, tem habilidades para dominar, monitorar, *hackear*, invadir, vigiar, acompanhar, 'olhar e observar' sistemas de informação e comunicação de terceiros, sem arriscar-se depois e, muitas vezes, com garantia de anonimato total. Se a traição, seja por temor às punições severas, seja por fidelidade à pátria, não figurava como estatística significativa entre as agências de inteligência durante a Guerra Fria, fosse porque tais números eram omitidos ou mesmo nem existissem, fosse porque eram manipulados, o mesmo parece não poder ser percebido hoje, quando o espião desloca-se de uma estrutura supersecreta e de uma hierarquia rigidamente controlada para um sistema no qual se vê como uma importante peça, mas apenas mais uma na engrenagem de uma máquina incapaz de disfarçar todas suas contradições.

Esse acesso irrestrito acaba por garantir ao espião contemporâneo acesso inclusive a práticas perniciosas da própria 'pátria', que agora passam a ser objeto de questionamento por parte daquele cuja responsabilidade não era refletir sobre si mesmo, mas sobre o comportamento do outro (o inimigo), instituído como alvo, ou adversário. Alça-se, então, o indivíduo a uma posição acima das maquiavélicas razões de Estado. Como no caso do espião da Alemanha Oriental Gerd Wiesler,[4] o sujeito que espiona, a partir de um olhar crítico sobre si mesmo, conflita sua atuação com sua moral, gerando uma crise que, se na Guerra Fria, poderia se manifestar na forma de depressão pessoal, na atualidade materializa-se em delações e revelações que se voltam contra a própria aparelhagem de espionagem, muitas vezes como efeito colateral do não atingimento de um objetivo maior, que seria desarticular toda a malha de relações encobertas. Não compõe, por evidente, o escopo deste trabalho buscar as motivações psicológicas, sociais, morais ou éticas que poderiam levar um espião ou alguém dotado de informações privilegiadas a cometer uma denúncia ou alcaguetagem, mas seria demasiado imprudente ignorar o fato de que já não existe exagerada rigidez na formação hermética e ideológica de um espião, como o foi, por exemplo, durante a Guerra Fria, sobretudo se tomamos em conta a geração atual de jovens espiões formados a partir de sua própria prática e experiência não institucionalizadas, como ilustra bem o próprio Edward Snowden.

Justamente porque o complexo e longo processo que envolve a segurança cibernética ou bancos de dados e sistemas de comunicação de uma nação apenas inicia-se (ou termina) com a espionagem, interessa-se aqui em buscar primeiro descrever como se deram os monitoramentos revelados por Snowden, no caso envolvendo o Brasil, em 2013, assim, além

[4] Gerd Wiesler, um agente da Stasi, a polícia política da República Democrática Alemã (Alemanha Oriental), envolveu-se num serviço de escutas clandestinas do apartamento de um casal da cena cultural de Berlim Oriental, o escritor Georg Dreyman e a atriz Christa-Maria Sieland. Mais tarde, ele se vê envolvido na vida do casal e tem um papel decisivo em poupar suas vidas.

dos endereços eletrônicos tradicionais e alternativos, optamos por dar prioridade às informações presentes em duas obras que julgamos essenciais no momento de escritura deste trabalho: 1) *Sem lugar para se esconder: Edward Snowden, a NSA e a espionagem do governo americano*, de Glenn Greenwald (2014); e 2) *Os arquivos Snowden: a história secreta do homem mais procurado do mundo*, de Luke Harding (2014). A partir daí, interessa-nos pensar em que medida a ideia de quebra de soberania brasileira foi evocada para na verdade sombrear certa ineficiência da contra-inteligência nacional, naqueles termos particularmente colocados por Cepik (esforços de obtenção de inteligência sobre as capacidades, intenções e operações dos serviços de inteligência adversário), bem como em que medida uma possível amenização ou solução do problema deva passar por ações unicamente nacionais ou concertadas com os vizinhos sul-americanos, por exemplo. Por meio da análise do caso Brasil x EUA queremos alargar a reflexão e pensar o próprio sistema internacional como uma grande rede marcada por um 'hardware' concreto e visível (marcado pelas desigualdades entre os Estados) e um 'software' abstrato e invisível (marcado pela força do capital financeiro), espaço justamente onde se é possível praticar a espionagem, cuja essência está obrigatoriamente condicionada a sua não ciência.

Localizar, portanto, a espionagem dentro dos estudos de segurança e defesa exige compreender tanto uma quanto outros e onde se interseccionam. A espionagem em si, embora ilegal, não se caracteriza essencialmente como prática marcada pela violência física (embora também o seja em muitos casos), logo, isolada, poderia parecer não abarcada pelos Estudos de Segurança Internacional (ESI), como o são a dissuasão para os Estudos Estratégico ou a prevenção para a Pesquisa da Paz.

Entretanto, a espionagem pode tornar-se, na verdade, um dos vários instrumentos por meio dos quais se viabilizam a segurança, reforçando-a, quando há sucesso (obtenção da informação; processamento e dedução de que não há riscos; com consequente não descoberta) ou tornando-a vulnerável e insuficiente quando há falha (a descoberta ocorre no ato de obtenção da informação). A espionagem pode, nesse sentido, ser entendida como o elemento (desencadeador) promotor ou regulador de violência, na medida em que suas 'descobertas' podem, quando percebidas como ameaças, gerar graves controvérsias (como a Crise dos Mísseis, em Cuba, evidenciada quando aviões espiões estadunidenses sobrevoavam a ilha), ou, quando percebidas como 'normalidade', ou seja, sem grandes consequências nem para o espionado nem para o espião, manter o *status quo* e a aparência de naturalidade da relação entre os envolvidos. A questão Snowden, portanto, deu visibilidade a uma realidade apenas aceita pelo seu caráter secreto. Uma vez que o segredo foi revelado, revelou-se junto que a

preocupação da superpotência (EUA) não se limitava exclusivamente a uma rede de possíveis futuros adversários, como seria o caso de China, Rússia ou União Europeia, mas também de atores considerados menos centrais no cenário internacional, como o Brasil, insinuando uma exagerada preocupação estadunidense não mais com quem seria a incógnita oposta de uma nova bipolaridade, mas com a manutenção da própria hegemonia e unipolaridade, além, claro, de fazer aparecer toda a hipocrisia e falsidade presente nas relações internacionais.

Por conta disso, então, é que se inclui a espionagem dentro dos Estudos de Segurança Internacional - ESI, pois está vinculada à geração ou precaução da violência e da paz. E, como tal, deve ser pensada à luz das quatro questões estruturantes dos ESI, nos termos em que coloca Buzan (2012), ou seja, 1) do privilégio do Estado como objeto de referência; 2) da inclusão tanto de ameaças internas quanto externas; 3) da expansão da segurança para além do setor militar e do uso da força; e 4) da compreensão da segurança como inextricavelmente ligada à dinâmica de ameaças, perigos e urgência. Além disso, refletir sobre espionagem impõe correlacionar conceitos complementares (dissuasão, estratégia, contenção), paralelos (poder, soberania, identidade) e opositores (paz, risco). Apesar de encaminharmos a reflexão passando tanto pelas 4 questões estruturantes quanto pelos 3 tipos de conceitos, nossa sustentação teórica escolhida, a Escola de Copenhague[5], focará a coletividade e o meio ambiente como objeto de referência de nossa pesquisa, assim como considerará os níveis internos e externos à nação, bem como todos os setores envolvidos (não só militar), a partir de uma visão de política de segurança neutra e de uma epistemologia que perpassa a análise do ato da fala, focando, portanto, mais as novas unidades da análise de segurança e a abordagem multissetorial da segurança, relacionadas à espionagem, e menos o conceito de securitização, embora sem ignorá-lo.

Como categorias de análises prioritárias, valer-nos-emos das ‘cinco forças’ elencadas por Buzan (2012): 1) a política das grandes potências, 2) a tecnologia, 3) os eventos, 4) os debates acadêmicos e 5) a institucionalização. Dentre as cinco, as que mais acabam ganhando destaque são as três primeiras e, dentre elas, a segunda ocupará mais nossa atenção, primeiro porque tanto a espionagem estadunidense ao Brasil quanto a descoberta dos respectivos

[5] A escola procura sintetizar correntes realistas e construtivistas da Teoria das Relações Internacionais, considerando que o estudo da segurança e/ou da insegurança deve englobar tanto aspectos materiais – armas, distribuição de poder, questões demográficas etc. – quanto imateriais próprios das fontes de insegurança. Os aspectos imateriais se referem a processos sociocognitivos de interpretação de ameaças inerentes à forma com a qual determinado assunto – não necessariamente relacionado ao emprego da força, como, por exemplo, o caso das migrações ou a degradação do meio ambiente – é enquadrado como ameaça existencial a um objeto de referência – a população do país que recebe migrantes, ou a humanidade, respectivamente, no caso dos exemplos citados anteriormente. (Cepik et al. (2014)).

monitoramentos materializaram-se por meio virtual; segundo, porque, segundo Buzan (2012), a tecnologia tornou-se essencial para a segurança por meio da revolução em assuntos militares (RAM), em especial pela utilização norte-americana de "vigilância global, comunicação em redes, armamentos inteligentes, aviões robôs, simulação em tempo real e o rápido estacionamento de forças especais", uma forma de guerra que gira em torno de "poucas baixas, longas distâncias e boa observação".

A tecnologia tornou-se fundamental também a partir de estudos que examinaram a utilização terrorista das tecnologias de rede e como a internet tinha se tornado um local de movimentos antiguerras/pacificistas, ao mesmo tempo que alvo de vigilância governamental. A importância do ciberespaço para infraestruturas críticas e para a construção de comunidades – incluindo grupos que combatiam regimes totalitários -, ressalta Buzan (2012), antecedia o 11 de Setembro pelo fato de o governo Clinton ter reconhecido a "cibersegurança" como uma questão nos anos 1990, mas a guerra contra o terror levou tal preocupação para um nível novo e mais complexo.

Sendo os EUA a gênese desencadeadora da temática circunscrita neste trabalho, faz-se necessário recordar sinteticamente sua história, buscando pontuar os principais aspectos correlacionados com a prática da espionagem, de modo que seja possível observar um *continuum* que em parte explica a preocupação estadunidense com ameaças externas e que em parte esclarece o componente inefável do 'destino manifesto' tão presente no ideário norte-americano. Nesse sentido, o próximo item discorrerá sobre o processo de formação dos EUA e como sua história influenciou – e influencia – o movimento deste Estado na política das grandes potências, além de descrever seus principais movimentos e ações em um sistema internacional que coloca em xeque a hegemonia da 'América'.

2. CONSIDERAÇÕES POLÍTICAS E ESTRATÉGICAS SOBRE A ESPIONAGEM

Este tópico, subdividido em duas partes, apresenta inicialmente a política dos EUA, ressaltando algumas passagens por meios das quais se observam a influência da espionagem na formação histórica norte-americana. Entremeiam-se na descrição histórica ações mais atuais, sugestivas da lógica hegemônica e supostamente imperialista dos estadunidenses, que passaram a desenvolver, então, uma percepção de que suas ameaças aumentaram em um cenário internacional caracterizado por um momento de transformação. A seguir, apresenta-se os principais acontecimentos que teriam influenciado as decisões de ampliação dos sistemas de monitoramentos do Estado norte-americano ao redor do mundo

2.1. POLÍTICA DAS GRANDES POTÊNCIAS – EUA

A contemporaneidade das relações internacionais tem sido marcada pelo debate sobre qual polaridade viria a substituir a bipolaridade após o fim da Guerra Fria, com extremos que vão da *uni* à *multipolaridade*. A ascensão da China, a reinserção da Rússia, a emergência dos BRICS, a relativa consolidação da União Europeia (institucionalizada, mas em crise), a desordem financeira, entre outros fatores, produzem um cenário internacional atual marcado por uma incógnita em relação ao domínio norte-americano, inquestionável a partir de 1990. É evidente que a percepção estadunidense de ameaça ao seu domínio veio a se refletir em posturas e decisões que iam da arrogância à imposição, da unilateralidade a práticas de monitoramentos. Essas práticas, bem como a preocupação excessiva com segurança quase se confundem com o estabelecimento dos EUA enquanto nação. Segundo Buzan (2012), uma característica que distingue os EUA é que sua geografia e sua história os isolaram dos rigores da guerra e do equilíbrio de poder em uma extensão muito maior do que a que teria ocorrido na maior parte dos países da Eurásia. Tal isolacionismo teria sido uma opção para os EUA de uma maneira que não foi para as outras potências, e os EUA, para Buzan (2012), têm fortes tradições contra emaranhados militares e compromissos com o exterior. Além disso, os EUA teriam como norma, para Buzan (2012), um padrão maior de segurança nacional: um desejo de estar

absolutamente seguros contra ameaças externas, como sua própria história cheia de exemplos pode perfeitamente ilustrar, assim como seu cinema, carregado de inimigos reais e inventados, terrenos e extraterrenos.

Esta alta expectativa por segurança pode, para Buzan (2012), ser vista também na resposta norte-americana ao 11 de Setembro: o choque da vulnerabilidade teria tingido em cheio os EUA, de uma maneira que fez com que sociedades com expectativas menos severas de segurança tivessem dificuldade de compreender ou simpatizar com ela. Karnal et al. (2007) advogam que o fim da Guerra Fria parecia ser a vitória histórica do modelo capitalista e liberal, mas que tal sonho de fim da História veio abaixo com as duas torres que tombaram. Os atentados, para Karnal et al. (2007), passaram a significar um contato doloroso dos EUA com o mundo, de modo que o mal distante, antes isolado no outro lado do mundo, parecia agora desfilar dentro de casa, fazendo paradoxalmente com que poucos norte-americanos pudessem estabelecer uma relação clara entre a política externa do país e os atentados. Uma hipótese que justifica tal postura dos estadunidenses poderia ser a de que, como querem Karnal et al. (2007), o outro adquire certa invisibilidade para os EUA, de modo que um inglês do século XIX olhava para o outro e dizia: "você é inferior"; o norte-americano do século XXI dificilmente reconhece a existência do outro a não ser no código eu/antieu. Esse comportamento corrobora que toda alteridade negativa - cuja construção, conforme elabora Sahd (2012), retoma características e símbolos existentes no imaginário coletivo - inventa novos símbolos e mitos, reforça preconceitos e delimita dois campos: um nós, os "normais", sujeitos cotidianos, e um eles, os diferentes, qualitativamente inferiores, que não querem e não devem ser como todos, portanto, os representantes da "não normalização".

Nesse escopo de 'inimigo a ser combatido', os 'terroristas' estão para os EUA como os palestinos estão para Israel. E em nome da segurança, todo tipo de violação, como a prática social genocida contra os palestinos, como a espionagem revelada por Snowden, como as guerras preventivas, são justificadas. Sahd (2012) reforça que no momento de construção da alteridade a violência contra o outro se manifesta por meio de imagens, que mais tarde justificarão a necessidade de combatê-los ou exterminá-los. O perigo, portanto, de aceitar como natural a prática ampla e sistemática da espionagem é exatamente ela se constituir no primeiro passo de um aparato rumo a um mundo distópico irreversível, organizado em torno de uma torre panóptica[6].

[6] Termo cunhado por Jeremy Bentham, filósofo e codificador britânico do século XVIII. Descrevia uma engenhosa prisão circular onde os guardas podiam ver os prisioneiros o tempo todo, sem que estes soubessem que estavam sendo observados. O termo é recuperado mais tarde por Michel Foucault (Vigiar e

Formando-se sem um cabresto inglês de um projeto colonial sistemático (a Inglaterra estava envolvida em conturbações internas), os EUA não tiveram a metrópole no encalço, fato que não gerou um referencial uniforme que norteasse a colonização. Além disso, tendo a Coroa inglesa entregado a particulares a atividade de colonização, os EUA vão nascendo a partir de companhias organizadas por comerciantes e que apresentavam todas as características de empresas capitalistas. Para Karnal et al. (2007), nesse caso, ao contrário da América ibérica, definiu-se uma colonização de empresa, não de Estado, o que explica ainda hoje a difusa relação entre interesses nacionais e interesses corporativos dos EUA (como se percebe no contencioso Brasil x EUA da informática, na década de 1980, a ser abordado proximamente no item 2.2).

Não obstante, junto com as companhias, que dariam o viés capitalista ao futuro país, a Inglaterra também influenciou e disseminou entre os colonizados a utilização da pena de morte, o que contribuiria para dar ao futuro país uma preocupação quase obsessiva com a segurança. É símbolo dessa obsessão a primeira execução registrada nas novas colônias: o Capitão George Kendall, da colônia de Jamestown, Virgínia, em 1608, foi executado por ser um espião para a Espanha; na sequência, então, em 1612, ainda na Virginia, o Governador, Sir Thomas Dale, promulgou as Leis Divinas, Morais e Marciais, que instituiu a pena de morte, mesmo para pequenos delitos, como roubar uvas, matar galinhas ou negociar com os índios. Durante a Primeira Guerra Mundial, a instituição do *Espionage Act* (Lei de Espionagem), de 1918, restringiu a liberdade de expressão, censurou jornais e proibiu qualquer atividade contrária aos objetivos do governo na guerra. Na Segunda Guerra Mundial, investigações dos serviços de inteligência dos EUA confirmaram que a comunidade de ascendência japonesa, 75% dos quais detinham cidadania, não representava nenhuma ameaça à condução da guerra.

Como se vê, a obsessão interna com a espionagem, aplicada severamente aos traidores, ironicamente acabaria por se tornar uma prática de Estado, institucionalizada via um complexo de agências de inteligência, especialmente a partir do século XX. Somou-se a essa rigidez securitária a ideia de povo eleito e especial diante do mundo, de modo que, como lembra Karnal et al. (2007), para manter a identidade e coesão do grupo, os puritanos exerceram um controle muito grande sobre todas as atividades dos indivíduos, gerando a ideia de uma moral coletiva onde o erro de um indivíduo podia comprometer o grupo, sendo o pacto Deus-povo com todos os eleitos.

Para Fiori (2007), apesar do caráter edificante e puritano do mito fundamental, na

---

Punir), para tratar de uma sociedade disciplinar, e pelos teóricos das novas tecnologias, como Pierre Lévy e Dwight Howard Rheingold, para designar o possível controle exercido pelos novos meios de informação sobre seus usuários.

contramão da tese da excepcionalidade, todas as evidências indicam que a economia norte-americana ocupou, a partir de sua independência, uma posição complementar e privilegiada com relação à economia inglesa, de modo que, no início, ao romper seus laços políticos com a Inglaterra, os Estados Unidos se tornaram uma periferia agroexportadora da economia britânica, mas, logo em seguida, se tornaram os maiores hospedeiros e beneficiários do capital financeiro inglês e dos seus investimentos diretos, sobretudo em serviços, transportes e comunicações. Em seguida, também seguiram o modelo da Inglaterra de Cromwell, durante sua Guerra Civil, entre 1861 e 1864, ou seja, ali se estabeleceram as bases fiscais, administrativas e militares do moderno Estado norte-americano, bem como se formaram, juntos, o sistema da dívida pública e o sistema de crédito de seus bancos, casando definitivamente o poder do Estado com o dos grandes capitais norte-americanos, união que se tornaria a verdadeira locomotiva de sua economia, entre 1870 e 1914.

Embora a independência das 13 colônias tenha sido marcada mais por um sentimento antibritânico que nacionalista, foi, também, segundo Karnal et al. (2007), fruto da luta de milícias, que eram grupos mais ou menos autônomos de colonos que faziam atos de sabotagem contra o exército inglês. Sabotagem aqui pode ser compreendida como uma 'prima' distante da espionagem. No século XIX, o sentimento nacionalista dos EUA começou a ganhar nova roupagem, sob a forma de conquistas territoriais, levando o país, nas palavras de Karnal et al. (2007), a partir da crença de que seu comércio era muito importante e totalmente necessário para os países da Europa, a tentar utilizar esse mesmo comércio como arma de guerra e moeda de troca em negociações. Simultaneamente, instituem a Doutrina Monroe para as Américas e vão se expandindo, justificando o imperialismo com 'civilização e progresso', 'democracia e liberdade' e, sobretudo, associando batalhas imperialistas contra indígenas e mexicanos às realizadas no processo de independência de 1776, pois, assim, garantiriam a paz em relação ao inimigo externo, lançando para bem longe toda e qualquer ameaça à soberania norte-americana.

Na Guerra de Secessão, a prática da espionagem também apareceu: Lincoln caminhava na direção de retomar as rédeas de todo o país, impedir a fragmentação do território e criar, se possível, uma unidade nas leis e na administração dos estados, para isso, no entanto, segundo Karnal et al. (2007), o governo agia de forma enérgica, violando correspondências, fechando jornais, prendendo sem julgamento e punindo os que desertavam do exército, tudo em nome da vitória da União, que, afinal, venceu o conflito e abriu caminho para o surgimento das grandes corporações, que caminhavam sempre no mesmo sentido monopolista (segundo Karnal et al. (2007), entre 1888 e 1905, foram formados 328 conglomerados ou empresas consolidadas). Volkman (2013) recorda que, em 1862, um general, Joseph Hooker, ordenou a criação do

Gabinete de Informação Militar, a primeira agência militar de inteligência na história dos EUA, que, sob a direção do chefe da polícia militar, coronel George H. Sharpe, tornou-se uma organização de inteligência de primeira classe, cujo triunfo supremo teria ocorrido em 1863, quando Sharpe preparou um relatório de nove páginas sobre o exército confederado, que planejava um ataque na Pensilvânia.

Entretanto, segundo Volkman (2013), quando a guerra civil eclodiu, nem a Uniao nem a Confederação tinham uma agência de inteligência de qualquer espécie e nenhuma organização de criptografria, sequer os militares tinham qualquer agente treinado, o que fez com que ambos os lados percebessem que iriam precisar de inteligência, mas, sem profissionais disponíveis, havia apenas um recurso: contratar amadores, ou seja, qualquer pessoa voluntariamente disposta a se tornar um espião (como foi o caso da espiã confederada Rose O'Neil Greenhow e da espiã da União Harriet Tubman). Conforme Volkman (2013), James D. Bulloch, um ex-oficial da Marinha dos EUA que se juntara à Confederação, após chefiar um programa de construção naval secreta dos confederados na Inglaterra, viu seu navio Alabama ser afundado por um navio da União; deprimido, teria dito: "Os espiões dos EUA são numerosos, ativos e inescrupulosos; eles invadem a privacidade das famílias, mexem com os clientes confidenciais de comerciantes e conseguiram converter uma parte da polícia de seu Reino em agentes secretos dos EUA". O ano era o de 1864.

Apesar disso, conforme Karnal et al. (2007), a maioria dos norte-americanos do período acreditava que seu país era a maior nação do planeta e que aquelas terras viviam em constante e 'natural' perigo diante de ameaças externas. O imperialismo empresarial estadunidense foi, então, mesclando a profética missão de ser guardião das instituições republicanas e democrática do Estado com o desejo corporativo de expandir o comércio exterior. Os EUA fizeram inúmeras intervenções nos assuntos internos de países do continente (Cuba, Haiti, República Dominicana, Nicarágua, México, Colômbia, por exemplo). Para Karnal et al. (2007), essa política externa era justificada pelo 'destino manifesto', sob a forma de anglo-saxonismo: a crença de que a nação norte-americana "anglo-teutônica" era superior do ponto de vista racial e tinha uma missão civilizatória a realizar, nesse sentido, o mundo estaria sendo beneficiado com a expansão, bem como a guerra manteria virtudes morais altas e os espíritos disciplinados, em pressupostos bem próximos aos do darwinismo social. E a espionagem teve papel fundamental no processo.

Bandeira (2010b) relembra que a CIA – já no século XX - forneceu todos aos armamentos-rifles, pistolas e metralhadoras - aos dissidentes que tencionavam, na República Dominicana, assassinar o ditador Rafael Trujillo, e a Casa Branca, bem como o Departamento

de Estado, souberam, antecipadamente, do crime, cometido com êxito, em maio de 1961. Complô igual, assinala Bandeira (2010b), foi planejado, simultaneamente, contra o ditador do Haiti, François Duvalier, conforme o próprio embaixador Adolf Berle Jr. teria revelado ao chanceler Afonso Arinos, ao visitar o Brasil, em fevereiro de 1961, ocasião em que Berle também teria pedido apoio brasileiro à invasão de Cuba, como parte de um movimento mais amplo, com o objetivo de 'restaurar a democracia representativa nos diversos países do continente'.

Internamente, no começo do século XX, os EUA avançam enormemente em tecnologia nos processos de produção na indústria automobilística, de comunicações, eletrônicos e plásticos, fato que estabeleceria uma dialética infinita com a indústria militar e que teria grande influência no melhoramento de técnicas de espionagem, especialmente a distância; além disso, a propaganda e as novas opções de lazer (cinema e esportes profissionais) suplantam a política como foco de preocupação pública, o que libera o Estado para agir com mais ousadia ainda, interna ou externamente, no que dizia respeito aos métodos de 'segurança'. Os EUA saem da Segunda Guerra Mundial como líder militar e econômico do mundo, com a economia sendo controlada mais do que nunca pelas grandes corporações e a política externa sendo definida pela agenda da segurança nacional e considerações imperialistas.

Durante a Guerra Fria, a 'paz' formal entre EUA e URSS, baseada na ameaça mútua das armas nucleares, resultou, segundo Karnal et al. (2007), na militarização da economia estadunidense, que passou a ser fortemente relacionada à produção de armas e outros produtos da guerra sob o controle do 'complexo militar-industrial'. Para Karnal et al. (2007), o mais alto padrão de vida no mundo foi baseado em grande parte nos gastos militares, que atingiram o pico de 20% da produção nacional durante a Guerra na Coréia. Na América Latina, a Guerra Fria se traduziu em manipulação da retórica anticomunista, com os EUA mantendo os países na esfera da influência ocidental por meio de invasão, orquestrações de golpes, obstáculos à reforma social e apoio técnico e político a regimes militares repressivos. O Departamente de Estado e a CIA, por exemplo, promoveram, planejaram e executaram a derrubada do governo reformista de Jacobo Arbenz na Guatemala, em 1954. Pillas (1996) recorda que dois dias depois de assumir o cargo, Ronald Reagan bloqueou a ajuda econômica destinada à Nicarágua, depois financiou e treinou o primeiro núcleo de somozistas que iria organizar a contra-revolução, e aumentou a ajuda militar à junta salvadorenha. Sua embaixadora na ONU, Jane Kirkpatrick, estabeleceu uma sutil distinção entre os regimes totalitários (comunistas), irreformáveis, e os regimes autoritários (ditaduras pró-americanas), suscetíveis de evolução democrática.

Desde o triunfo da revolução sandinista na Nicarágua e o desenvolvimento da guerrilha

em El Salvador e na Guatemala, a administração Reagan, para Pillas (1996), preocupada com o papel representado por Cuba na unificação dos movimentos revolucionários, fez tudo o que esteve em seu poder para confinar de novo Havana em seu isolamento. Reagan devolveu à CIA o lugar preponderante que ocupou nos anos 50. Depois das revelações sobre o envolvimento da CIA no sangrento golpe de Estado chileno (1973), a emenda Hugh-Ryan, de 1974, reduziu os serviços secretos praticamente à impotência, obrigando-os, antes de conduzir operações clandestinas no exterior, a obter sinal verde do presidente e avisar os 163 membros das comissões responsáveis do Congresso. Mas nem mesmo tal emenda refreou a sanha por espionagem: Reagan escolheu como vice-presidente George Bush, um antigo diretor da CIA, e nomeou, à frente da Agência, William Casey, um amigo íntimo, membro da Ordem de Malta.

Bandeira (2010b) registra que logo depois do golpe de Estado no Chile (1973), com o conhecimento da CIA, os serviços de inteligência do Chile, Argentina, Brasil, Paraguai e Uruguai passaram a cooperar e, em 1975, instituíram a Operação Condor, codinome dado ao acordo para o empreendimento de açoes conjuntas, visando a coordenar a repressão e eliminar os adversários dos regimes ditatoriais existentes nos países do Cone Sul. Ainda segundo Bandeira (2010b), o raio de ação da Operação Condor não se restringiu à América Latina: a terceira fase e a mais secreta da Operação Condor [segundo o documento desclassificado pelo Defense Intelligence Agency (DIA), do Exército norte-americano] consistiu em formar equipes especiais dos países membros a fim de que viajassem por todo o mundo e executassem sanções, que incluíam assassinatos contra supostos terroristas ou que apoiassem suas organizações, ou seja, contra adversários políticos dos regimes militares instalados no Cone Sul; se um adversário político ou um que apoiasse a organização política adversa estivesse na Europa, uma equipe especial da Operação Condor seria enviada para o localizar e vigiá-lo; quando culminasse a localização e a vigilância, uma segunda equipe da Operação Condor seria enviada para aplicar a sanção efetiva contra aquele adversário; assim, teoricamente, um país proveria de documentação falsa a equipe de assassinos, formada por agentes de um outro país.

No plano interno estadunidense, as coisas não foram diferentes; o Macartismo foi uma campanha contra a subversão em todos os aspectos da vida americana: investigações contra a suposta subversão de intelectuais, artistas e funcionários resultaram em inúmeras demissões, centenas de sentenças de prisão e algumas execuções (como o já citado casal de comunista Julius e Ethel Rosenberg). Mesmo depois do fracasso no Vietnã, os EUA mantiveram sua postura imperialista, intervindo em vários países para impedir ameaças a sua hegemonia

político-econômica [7]. Seu principal objetivo sempre foi o de abrir oportunidades de investimento às corporações americanas, utilizando seu vasto poder econômico e militar para controlar países e conter a ameaça de inimigos, que, na Guerra Fria, eram a URSS e, por ora, nas palavras de Karnal et al. (2007), a figura do 'terrorista' parece preencher bem a necessidade historicamente permanente do inimigo constituído.

Para Bandeira (2010a), o 'perigo verde', identificado com o fundamentalismo islâmico, começou a substituir o 'perigo vermelho', representado pela URSS, e o 'terrorismo internacional' passou a ocupar relevante espaço na agenda internacional dos EUA, que, também, após o fim da URSS e de todo o bloco socialista, inseriram o narcotráfico como inimigo a combater. Dessa forma, por meio do poder militar, com o suporte da mídia, como as redes de televisão CNN e Fox, os EUA passatram a dominar o mundo e conformaram, segundo Bandeira (2010a), um império informal, a partir da derrota da Alemanha e do Japão, em 1945. Com a ascensão de Bush filho, a mudança na estratégia de segurança nacional dos EUA substituiu a doutrina de contenção e dissuasão pela de ataques preventivos. A segurança nacional dos EUA implicava, neste sentido, o domínio das fontes de energia, no Oriente Médio, onde estão depositadoas cerca de 64,5% das reservas conhecidas de petróleo, bem como na Ásia Central.

Nessa política das grandes potências, segundo Bandeira (2010a), os objetivos estratégicos dos EUA e da União Europeia (EU), na Ásia Central, colidem com os interesses geopolíticos da Rússia, que se sente gravemente afetada com o avanço da OTAN. E, a despeito de disporem ainda de meios para intervir imediata e efetivamente em qualquer região do mundo, Bandeira (2010a) considera que o Império Americano evidencia certo declínio, tanto no nível econômico como político militar, já que, economicamente, estão a depender pesadamente do influxo de capitais de outros países, sobretudo da China, e militarmente, têm tido dificuldade de recrutar jovens para servir como soldados nas Forças Armadas, especialmente depois da invasão do Iraque e a desgastante permanência no solo invadido.

Vizentini (2004) acredita que muitos viram nas ações político-militares unilaterais da administração Bush uma retomada do poder americano, configurando uma nova hegemonia "unipolar" para o século XXI, que, como o anterior, seria novamente americano, ou então um

[7] O caso cubano é o mais ilustrativo: sogata do arroz, peste suína africana, doença de Newcastle das aves domésticas, carvão e ferrugem da cana-de-açúcar, mofo azul do tabaco, dengue, conjuntivite hemorrágica e ferrugem do café – todas estas doenças, surgidas na Ilha de 1971 a 1986, e que ocasionaram numerosas mortes e consideráveis perdas econômicas, são altamente suspeitas aos olhos das autoridades cubanas (Pillas, 1996). A postura estadunidense com Cuba no período lembra a atual de Israel com a Palestina.

caos geral, com o mundo mergulhando numa espécie de "guerra dos cem anos" religiosa (ou civilizacional). Segundo Vizentini (2004), na verdade, trata-se de uma reação para evitar uma tendência histórica que emerge lentamente: a de construção de um sistema mundial multipolar, num quadro de equilíbrios entre EUA/NAFTA, União Europeia, Rússia/CEI, Japão/Tigres Asiáticos, China, Índia, Irã, África do Sul/SADC e Brasil/Mercosul (como teria assinalado o politólogo brasileiro Hélio Jaguaribe). Para Vizentini (2004), como os blocos econômicos constituem o principal resultado da globalização, e estão se tornando blocos político-econômicos, os EUA temem a formação de uma constelação eurasiana que, por seu peso econômico, militar e demográfico, torne a América uma periferia envelhecida dentro do sistema mundial, fazendo os polos emergentes tenderem a construir um sistema mundial multipolar, com equilíbrios de poder de geometria variável, onde as organizações multilaterais como as Nações Unidas ganhariam novo vigor, reformadas devido ao estabelecimento de uma nova correlação de forças. Dessa forma, a intervenção no sul da Eurásia, com o objetivo geopolítico de obstaculizar a formação de um megaespaço econômico, desarticular os "impérios continentais" que ressurgem e controlar as fontes produtoras de petróleo, constituiria um objetivo dificilmente alcançável para a "potência marítima" norte-americana.

Para Bandeira (2010a), estaria em curso uma Segunda Guerra Fria, mas os EUA dificilmente teriam condições de sustentá-la, em virtude do colapso do seu sistema financeiro. Nesse contexto, embora a América Latina seja, nas palavras de Samuel Pinheiro Guimarães[8], a zona estratégica mais importante para os EUA, é a América do Sul, nas palavras de Bandeira (2010a), a região que apresenta maior significação geopolítica devido ao seu enorme potencial econômico e político. Não teria sido, portanto, à toa o projeto da ALCA, bem como não teria sido coincidência, na sequência, sua rejeição pelo Brasil e, nos anos 2000, a busca por uma identidade própria sulamericana (CASA, depois UNASUL). Pelos seus recursos energéticos e econômicos, é o Pentágono, segundo Bandeira (2010a), que determina e dirige a política exterior dos EUA com respeito à América do Sul, já que a Venezuela é o quarto maior exportador de petróleo para os EUA; Venezuela, Bolívia e Equador possuem importantes reservas de gás e petróleo; e Brasil, Colômbia, Argentina e Peru também produzem gás e petróleo. Entretanto, para Bandeira (2010a), de todos esses países, apenas o Brasil tem o potencial de tornar-se significativo produtor mundial de petróleo, na próxima década, com a exploração das jazidas encontradas na região do pré-sal, descobertas em águas profundas.

---

[8] Agência Carta Maior, 12/07/2012. "**Estados Unidos, Venezuela e Paraguai".**

Fiori (2007) observa que está em curso um nova ‘corrida imperialista’ entre as grandes potências, que lutam por sua segurança energética e alimentar. A China penetra cada vez mais na África, onde os países da UE buscam conservar a preeminência sobre suas antigas colônias. E a competição, como prevê, Fiori (2007), se já não atingiu, deverá atingir a América Latina. Os casos de monitoramento dos EUA no continente de forma geral e no Brasil de forma específica insinuam que sim. O Brasil teria interesses de sobra aos EUA: quase 200 milhões de habitantes, cerca de 8,5 milhoes de km² de extensão territorial, litoral de mais de 7 mil km, mais de 15 mil km de fronteiras sem litígio, terras férteis para a agricultura, reservas imensas, jazidas de ferro e outros minerais metálicos, urânio, biodiversidade, enormes reservas de água e recursos hidroelétricos, além de uma participação ativa do Brasil em processos de integração do continente, sem a participação dos EUA, bem como inserção em grupos de emergentes como o IBAS e o BRICS.

Para Lucas Kerr (2013), na atualidade, poucos blocos regionais apresentam o potencial propiciado pela concomitância de três elementos geopolíticos: (I) a possibilidade de que a região venha a se tornar uma região insular ou ilha-continente; (II) o elevado potencial para a integração da infraestrutura energética e logística regional, através das bacias hidrográficas, sendo estas nascentes no *Heartland* geopolítico do continente; (III) a perspectiva de que o processo de integração transforme a região em uma zona bioceânica, ou seja, com acesso simultâneo a dois grandes oceanos. A possibilidade de agregar estas três características geopolíticas existe justamente no caso da integração sul-americana, centrada geopoliticamente no Mercosul.

Para Fiori (2007), o assessor de segurança nacional de Clinton, Samuel Berger, teria tido razão quando disse que os EUA hoje controlam o acesso às redes de informações, comércio e segurança e, com isso, influenciam as escolhas das nações. Após a Guerra Fria, para Fiori (2007), teria havido uma transformação radical nos dois pilares em que todos os impérios sempre se sustentaram: o poder das armas e do dinheiro; e, após o 11 de Setembro, a Doutrina Bush de combate ao terrorismo teria transformado o interesse nacional norte-americano no princípio legitimador de um novo tipo de intervencionismo político-militar que se propõe permanente, preventivo e global. Para Fiori (2007), logo depois do 11 de Setembro, teria sido desengavetada uma proposta elaborada por Dick Cheney, ainda sob o governo de Bush pai, caracterizada pela lógica expansiva e truculenta que marcou a era de Bush filho, cujos objetivos eram impedir o aparecimento, em qualquer ponto do mundo, e por um tempo indefinido, de qualquer outra nação ou aliança de nações que pudessem se transformar em uma grande potência, capaz de rivalizar com os Estados Unidos. O problema, para Fiori (2007) foi que a

natureza invisível e onipresente do ‘novo inimigo’ permitiu uma redefinição estratégica sutil, mas absolutamente cruel: poderia ser o ‘desconhecido, o incerto, o inesperado’; poderia ser uma ameça vinda do espaço e ser nuclear, mas também poderia ser cibernética, biológica, química e poderia estar no ar, na terra, na água, nos alimentos, enfim em centenas de veículos ou lugares diferentes, porque seria pouco provável que alguém quisesse rivalizar ou competir com os EUA numa guerra convencional. Vizentini (2004) crê que o ‘terrorismo’ trata-se de uma gigantesca orquestração, manipulando o sentimento de insegurança das populações, numa época de crise e incertezas, sendo seu objetivo criar um consentimento a medidas repressivas que, em essência, implicam perseguição de opositores, simplesmente rotulados de ‘terroristas’, o que justificaria a supressão de direitos civis e o desencadeamento de guerras, constituindo, em verdade, dois grandes perigos: o terror coletivo empregado nas guerras civis e o terror virtual, utilizado para provocar um estado de tensão global que justifique certos propósitos políticos por parte de governos. Essa paranoia, segundo Fiori (2007), é o que explica um ponto estranho do plano contra ataques terroristas, enviado ao Congresso por Bush filho, em junho de 2002, propondo a criação de ‘equipes vermelhas’ que planejariam ataques contra os EUA, pensando como terroristas, para revelar os pontos fracos da segurança norte-americana.

Para Fiori (2007), os EUA, nessa ‘escalada aos extremos’ clausewitziana, teriam chegado ao limite da loucura com o desaparecimento de adversários competitivos e estariam se transformando em inimigos de si mesmos. Seria por isso, então, que, para Fiori (2007), essas características do novo inimigo dos EUA anunciam de imediato algumas dificuldades e limites no caminho da nova estratégia de contenção norte-americana: 1) uma vez que tudo pode se transformar em arma, em particular as inovações tecnológicas dos próprios norte-americanos e tudo pode se tranformar em alvo, em particular as coisas mais prezadas pelos EUA, então há a necessidade, defendida por Bush filho, de uma ‘rede cidadã’ de espionagem, construída por milhões de homens e mulheres comuns que gastariam parte de seus dias controlando e vigiando seus próprios vizinhos, o que levaria a exigir um controle permanente e cada vez mais rigoroso da própria sociedade norte-americana, vista pelo governo como um imenso universo de possibilidades agressivas; 2) uma vez que, do ponto de vista da segurança externa dos EUA, a nova estratégia cria uma situação de insegurança coletiva e permanente dentro do sistema mundial, já que o inimigo não é, em princípio, um religião, ideologia, nacionalidade, civilização ou Estado e pode ser redefinido a cada momento pelos próprios EUA, sendo, portanto, variável e arbitrário, os EUA, então, se guardam o direito de fazer ataques preventivos contra todo e qualquer Estado onde eles considerem existir bases ou apoio às ações terroristas, o que significa a auto-atribuição de uma soberania imperial, criando uma situação de guerra permanente, pronta

para ser declarada quando os EUA se considerarem ameaçados, no curto, médio ou longo prazo.

Nesse quadro, como nos lembra Fiori (2007), a necessidade norte-americana de alianças e apoios nas guerras do Afeganistão e do Iraque acabou devolvendo, recentemente, a liberdade de iniciativa militar ao Japão e à Alemanha, ao mesmo tempo permitiu à Rússia reinvidicar de volta seu direito de 'proteção' em sua 'área de influência' ou 'zona de segurança' clássica (vide caso atual da Ucrânia), onde se instalaram bases e tropas norte-americanas depois de 1991. Aos poucos, segundo Fiori (2007), está se formando uma nova polarização dentro do Oriente Médio com o surgimento de um eixo de poder xiita e a possibilidade de um confronto generalizado com as forças sunitas, dispersas por vários Estados da região (vide caso atual do Estado Islâmico). E, até mesmo na América Latina, podem-se, segundo Fiori (2007), identificar mudanças significativas na política externa de vários países que contestam ou propõem redefinir os termos da hegemonia norte-americana no 'hemisfério ocidental' (vide o caso atual da UNASUL). Em paralelo, do outro lado do mundo, o sistema estatal e capitalista asiático se parece, segundo Fiori (2007), cada vez mais com o bem-sucedido modelo do 'milagre europeu'.

Ainda segundo Fiori (2007), não é um desatino prever uma aliança crescente entre o poder econômico alemão e o poder militar 'ocioso' da Rússia, antigo pesadelo geopolítico dos anglo-saxões que, ao tornar-se realidade, pode redesenhar radicalmente a estrutura de poder dentro da massa eurasiana, bem como, por outro lado, a nova relação entre os EUA e China pode reproduzir e prolongar o eixo Europa-Ásia que dinamizou o sistema estatal e capitalista desde sua origem com a relação privilegiada dos EUA-Japão, a partir de 1949; nesse caso, entretanto, além da relação econômica complementar e competitiva entre os EUA e China, o próprio sucesso da relação econômica chinesa prenuncia uma disputa cada vez maior pela hegemonia militar no Sudeste Asiático. Para Fiori (2007), neste momento, os EUA não têm mais como se desfazer economicamente da China, mas chegará a hora em que os EUA terão de bloquear o movimento expansivo da China para fora se si mesma, no momento em que esse movimento não for mais apenas econômico e assumir forma de uma vontade política imperial. E o mesmo acontecerá, segundo Fiori (2007), caso se materialize uma aliança de longo prazo, econômica e militar, entre Alemanha e Rússia.

Nesse sentido, quadro pior para os EUA nao poderia existir num futuro em que o Brasil, clássico 'quintal' estadunidense, compusesse um bloco econômico, estratégico e militar com Rússia e China, no grupo dos BRICS, primeiro, porque o Brasil e a África do Sul compartem com China e Índia o fato de serem os Estados e as economias mais importantes de suas respectivas regiões, responsáveis por uma parte expressiva da população, do produto e do comércio interno e externo da América do Sul e da África; segundo, porque, a despeito de Brasil

e África do Sul não terem disputas territoriais com seus vizinhos, não enfrentarem ameaças internas ou externas à sua segurança e não serem potências militares relevantes, China e Índia se projetam dentro do sistema mundial como potências econômicas e militares, têm claras pretensões hegemônicas em suas respectivas regiões e devem seguir os passos de todas as grandes potências que fazem, ou já fizeram parte do 'círculo dirigente' do sistema mundial. É nesse contexto da política das grandes potências, cujo foco maior neste trabalho se debruça nos EUA, que devem ser compreendidos os monitoramentos denunciados por Snowden em 2013. A ordem mundial parece estar em transformação e os casos de espionagem, a despeito de sua histórica inserção na política externa dos EUA (como demonstramos), denunciam certa insanidade – e por isso mesmo, cada vez mais alto grau de periculosidade - da potência em começar a se perceber decadente. O item a seguir mostra a influência que alguns eventos puderam ter na vigilância global dos EUA.

2.2. EVENTOS

É difícil imaginar a evolução da espionagem sem o impacto de eventos-chave, mas, conforme lembra Buzan (2012) a propósito dos Estudos de Segurança Internacional, é igualmente importante que este impacto seja teorizado de modo que não afirme que os eventos são uma força causal que simplesmente exerce seu poder sobre uma comunidade acadêmica flexível. Assim, é necessário teorizar sobre esses eventos de uma maneira construtivista e enfatizando a interação entre eles e as outras forças motrizes (a Política das Grandes Potências [já trabalhado no subitem anterior], a Tecnologia [a ser abordada em 2.3], o Debate Acadêmico e a Institucionalização [que serão abordados subsequentemente, em 2.4]).

Para Buzan (2012), os eventos aparecem de várias formas e podem mudar não apenas as relações entre as potências, mas os paradigmas acadêmicos utilizados para compreender essas relações. As mais dramáticas, nesse sentido, são as crises específicas, que não só se tornam objetos de estudo por direito próprio, mas também mudam os entendimentos existentes, as relações e as práticas no domínio estratégico amplo. Nesse escopo podem ser inseridos, para o caso dos monitoramentos que nos interessa, principalmente a queda do *World Trade Center*, em 2001, mas também, como encadeamento histórico, a Primeira e Segunda Guerras Mundiais de forma geral, e a Guerra Fria de forma particular; dentro da Guerra Fria, a Guerra da Coréia, em 1950, a Crise dos Mísseis de Cuba, em 1962 e a Guerra do Vietnã, entre 1955 e 1975. O

próprio fim da Guerra Fria, com a dissolução da URSS (entre 1989 e 1991) tornou-se um evento decisivo para compreender a maneira como os serviços de inteligência norte-americanos encaminhariam suas práticas num mundo marcado pela unipolaridade. Na prática, para Fiori (2007), isso quis dizer que a administração Clinton seguiu as mesmas ideias básicas do governo Bush pai, os dois igualmente convencidos de que o século XXI seria um 'século norte-americano', como afirmou Bush, e de que o 'mundo necessitava dos EUA', como costumava repetir Madeleine Albright, a secretária de Clinton. Fiori (2007) lembra que o governo Clinton manteve um ativismo militar sem precedentes durante seus dois mandatos e que, segundo relatório da *US Comission on National Secutity*, de 1999, durante a era Clinton os EUA se envolveram em 48 intervenções militares, muito mais do que em toda a Guerra Fria, período em que ocorreram 16 intervenções. Estão no currículo de Clinton os ataques à Somália, em 1992 e 1993, o bombardeio do Sudão, em 1998, a Guerra do Kosovo, na ex-Iugoslávia, em 1999 e o bombardeio quase constante do Iraque, entre 1993 e 2003, além do anúncio, feito por Clinton em fevereiro de 1998, ao lado do então primeiro ministro inglês Tony Blair, da nova Guerra do Golfo ou do Iraque, que acabou protelada até 2003.

Outros eventos, para Buzan (2012), assumem a forma de processos constantes que se desdobram ao longo do tempo e mudam o conhecimento, o entendimento e a consciência que sustentam as práticas existentes. Nesse escopo, podemos inserir aqueles elencados por Fiori (2007): A) a derrota militar norte-americana, no Sudeste Asiático, que levou o meio acadêmico e a imprensa mundial a falar, nos anos 1970, em uma 'crise da hegemonia americana'; B) a restauração conservadora iniciada nos EUA na administração Nixon e disseminada pelo mundo depois das vitórias eleitorais de Thatcher e Ronald Reagan, provocando uma convergência no campo das ideias e das políticas econômicas que consagrou o neoliberalismo; C) a globalização em sua vertente econômica, cujo produto final é o surgimento, nos anos 1990, de uma finança mundial privada e desregulamentada por onde circula e se acumula uma riqueza rentista que já está, segundo Fiori (2007), na ordem de três a quatro trilhões de dólares; D) a revolução tecnológica [que analisaremos mais detalhadamente no próximo subitem], cujas invenções e descobertas fundamentais ocorreram durante a Segunda Guerra Mundial, mas cuja utilização econômica só aconteceu a partir da crise econômica dos anos 1970 e que pode ser vista no campo da microeletrônica, dos computadores e da telecomunicação e na espetacular influência da extensão, custo e velocidade de circulação das informações, facilitando e provocando alterações produtivas e gerenciais; E) o campo do trabalho e do emprego, que, após 25 anos de alto crescimento, foi afetado pela crise dos anos 1970, seguida das políticas deflacionistas e das mudanças tecnológicas, que provocaram a desaceleração do crescimento e uma reestruturação

produtiva que atingiu pesadamente o mundo do trabalho, do ponto de vista do número de empregos, de sua remuneração, da sua organização sindical e dos direitos sociais e trabalhistas; e, por fim, F) a transformação ocorrida no espaço da periferia capitalista, como resultado da crise econômica mundial que se alastrou a partir dos países centrais, desde o fim do Sistema de Bretton Woods e atingiu as principais economias periféricas, que enfrentaram, nos anos 1980, como consequência, uma crise generalizada de balanço de pagamentos.

No âmbito deste trabalho, em termos analíticos, temos em mente que os eventos serão, de fato, política e intersubjetivamente construídos, pois estamos partindo do princípio de que o reconhecimento (ou não) por parte de políticos, instituições, da mídia e do público de que algo é de tal importância que deveria ser dada uma resposta, mesmo que, possivelmente, por meios militares, é que faz disso um 'evento'. Partindo desse princípio e da divisão de eventos proposta por Buzan (2012), podemos considerar, conforme já mencionado, como um *evento constitutivo* do agravamento da prática de espionagem estadunidense, cujo resultado foi os monitoramentos aplicados no Brasil em 2013, a queda das torres gêmeas, em 11 de setembro de 2001.

A partir daí, como afirma Fiori (2007), não há dúvida de que, logo depois de sua posse, em janeiro de 2001, os primeiros passos externos da administração Bush pareciam apontar para um novo período de isolacionismo arrogante e exemplar, mas que foi após o 11 de setembro que a Doutrina Bush de combate ao terrorismo transformou o interesse nacional em intervencionismo global e preventivo. Para Bandeira (2010a), o 11 de Setembro e a consequente guerra ao terrorismo constituíram mera figura de retórica, um eufemismo para disfarçar os reais objetivos do presidente George W. Bush, que consistiam em vencer a resistência e/ou insurgência islâmica e controlar a Ásia Central e o Oriente Médio, com suas enormes jazidas de gás e petróleo, pautando a sua política internacional a convergência das necessidades da economia mundial capitalista e os interesses das grandes corporações. No caso em que nos ocupamos, como *evento critico significativo*, ou seja, aquele que, segundo Buzan (2012), é colocado na agenda devido a pressões da mídia ou iniciativas políticas, ressaltamos o duro ataque militar russo desfechado em agosto de 2008 contra as forças da Geórgia, que invadiram a região separatista da Ossétia do Sul, constituindo séria advertência de que aquela região, no Cáucaso, à margem do Mar Negro, estaria na esfera de influência da Rússia, que não permitiria maior penetração dos EUA e das potências industriais do Ocidente.

Ainda como *evento crítico significativo*, responsável pela mudança de percepção dos EUA em relação ao Brasil, é o início de uma consolidação do Brasil como potência regional na América do Sul. Para Bandeira (2010a), o aspecto econômico-comercial certamente pesou na decisão americana de reativar a IV Frota no Atlântico Sul, com a perspectiva de que a região se

torne um dos grandes centros produtores de petróleo, em virtude das recentes descobertas de jazidas, na camada pré-sal no litoral de São Paulo e que provavelmente se estendem por todo o sul até o litoral da Argentina. Para Bandeira (2010a), o envolvimento do Brasil, que mais e mais se projeta como potência econômica e política, desperta preocupação nos EUA: o Brasil é o maior exportador mundial de alimentos, podendo, brevemente tornar-se um dos maiores exportadores de petróleo, além disso possui grande parte do Aquífero Guarani, como boa parte das águas do Amazonas e boa parte da biodiversidade existente na região. Não obstante, como lembra Bandeira (2010a), o Brasil, ao encorajar o lançamento da União Sul-Americana de Nações, depois denominada União de Nações Sul-Americanas (UNASUL), teve um objetivo estratégico, visando a tornar não propriamente a si, mas o conjunto dos países do subcontinente uma potência mundial, não só econômica, mas também política. Combinada com a participação nos BRICS, que aproxima, via Brasil, a América do Sul de Rússia e China, aumentando a percepção de ameaça dos EUA em relação a geopolítica de uma Segunda Guerra Fria em sua própria área de influência, a integração sul-americana, via UNASUL, simultaneamente coloca, então, em xeque a hegemonia estadunidense no continente ao enfraquecer a OEA, bem como causam tensão nos norte-americanos o quadro de interdependência econômico-financeira que têm com a China e o choque de interesses geopolíticos que vêm travando com a Rússia, especialmente no Cáucaso, no Oriente Médio e, mais recentemente, na Ucrânia.

Como *evento crítico deferido*, ou seja, aquele que Buzan (2012) considera constituído como significativos por outros atores políticos, midiáticos ou acadêmicos, mas que uma teoria prefere ignorar ou categorizar como não fazendo parte de seu escopo, em nosso caso, podemos inserir a Batalha de Seattle, quando, em 30 de novembro de 1999, entre 40 e 100 mil manifestantes confrontaram os líderes do mundo industrializado na reunião da OMC, para protestar contra desequilíbrios da crescente globalização da economia. Antecedendo o 11 de Setembro, a batalha de Seattle foi importante pelo fato de agregar perspectivas distintas de vários setores da sociedade civil organizada: enquanto membros de ONGs e humanistas se envolveram como forma de protestar contra o avanço das políticas neoliberais, que consideravam uma ameaça aos direitos humanos e às políticas de saúde, educação e distribuição de renda nos países mais pobres, na ótica dos ambientalistas o encontro tinha como objetivo barrar as negociações da OMC, chamando a atenção para a degradação ambiental resultante das políticas desenvolvimentistas estatais e privadas; na ótica dos sindicalistas era o momento de lutar pela manutenção dos direitos trabalhistas; para diversos grupos anarquistas a reunião se mostrou uma ocasião para demonstrar o repúdio ao capitalismo global tanto pelas questões sociais como pelas questões ambientais, através de diferentes formas de ação direta.

A Batalha de Seattle é considerada em certos meios como uma manifestação superior a muitas outras ocorridas nos EUA, perdendo apenas para as manifestações contra a Guerra do Vietnã. Os acontecimentos em Seattle ganharam importância histórica como o marco inicial do movimento pela *altermundialização*, alternativo à globalização corporativa neoliberal, considerada nociva não só por este movimento. Em nosso caso, interessa-nos primeiramente ressaltar a importância da Batalha de Seattle na influência do cenário internacional, na medida em que ela se consolidou como resistência da sociedade civil organizada frente às corporações transnacionais e inspirou outras manifestações ao redor do mundo, quase sempre ignoradas pelas teorias *mainstream*. Segundamente, pela razão de a Batalha de Seattle ter dado origem à Mídia Independente, que mais tarde influenciaria o surgimento do WikiLeaks, outro *evento crítico deferido* que consideramos crucial para a compreensão da revelação, por Snowden, dos monitoramentos feitos pelos EUA no Brasil em 2013.

A indignação com o que consideravam uma cobertura distorcida dos meios de comunicação convencionais sobre as manifestações de Seattle levou anarquistas e ativistas com conhecimentos tecnológicos a criarem durante os protestos o projeto Indymedia[9].O objetivo era o de oferecer uma cobertura jornalística alternativa aos acontecimentos que apareciam nos meios de comunicação convencionais. Essencialmente seria veiculada pela internet e constituída colaborativamente por qualquer um que se voluntariasse. O projeto original consistia em um *website* para a publicação livre, no qual diferentes órgãos de imprensa alternativa publicariam relatos, entrevistas, análises e imagens em *copyleft* [um acordo por meio do qual um programa ou trabalho artístico pode ser usado, modificado e distribuído livremente na condição de que qualquer coisa derivada dele está vinculada à mesma condição], promovendo o intercâmbio de informações e a cooperação mútua.

Durante os protestos [de Seattle], no entanto, não apenas jornalistas independentes, mas os próprios ativistas se manifestaram, publicando seus pontos de vista, fotos e depoimentos. A junção da cobertura dos meios jornalísticos independentes com os relatos diretos dos participantes provocou um crescimento do *site*, com mais de um milhão de acessos. Como consequência do êxito alcançado nas comunicações durante os protestos de Seattle, rompendo o suposto cerco midiático, o projeto Indymedia, que era temporário, transformou-se numa iniciativa permanente. Em 2002, já existiam 89 sites do Indymedia em 31 países e em janeiro de 2006 já eram 150 sites. Atualmente o Indymedia constitui uma das maiores redes globais

[9] As informações sobre o Indymedia e sobre o WikiLeaks foram tiradas de seus próprios endereços eletrônicos (http://indymedia.org/ e http://wikileaks.com) – bem como do *site* http://wikipedia.org.

voluntárias e horizontais de notícias capaz de rivalizar com as coberturas de grandes conglomerados midiáticos na divulgação de informações.

Em 2006, sob o nome de WikiLeaks, surgiu uma organização transnacional sem fins lucrativos, sediada na Suécia, que publicou, em sua página (*site*), postagens (*posts*) de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis. A página foi construída com base em vários pacotes de programas (*software*), incluindo MediaWiki, Freenet, Tor e PGP (Pretty Good Privacy). Apesar do seu nome, a WikiLeaks não é uma *wiki*, ou seja, leitores que não têm as permissões adequadas não podem editar o seu conteúdo. A página, administrada por *The Sunshine Press*, foi lançada em dezembro de 2006 e, em meados de novembro de 2007, já continha 1,2 milhão de documentos. Seu principal editor e porta-voz é o australiano Julian Assange, jornalista e *ciberativista* (colega de Edward Snowden).

Ao longo de 2010, o WikiLeaks publicou grandes quantidades de documentos confidenciais do governo dos Estados Unidos, com forte repercussão mundial. Em abril do mesmo ano [2010], divulgou um vídeo de 2007, mostrando o ataque de um helicóptero Apache estadunidense matando pelo menos 12 pessoas - dentre as quais dois jornalistas da agência de notícias Reuters - em Bagdá, no contexto da ocupação do Iraque. O vídeo do ataque aéreo em Bagdá (*Collateral Murder*) é uma das mais notáveis publicações da página. Outro documento polêmico mostrado pela página é a cópia de um manual de instruções para tratamento de prisioneiros na prisão militar estadunidense de Guantánamo, em Cuba. Em julho ainda de 2010, o WikiLeaks promoveu a divulgação de uma grande quantidade de documentos secretos do exército dos Estados Unidos, reportando a morte de milhares de civis na guerra do Afeganistão em decorrência da ação de militares norte-americanos. Finalmente, em novembro de 2010, publicou uma série de telegramas secretos enviados pelas embaixadas dos Estados Unidos ao governo do país.

O que o WikiLeaks demonstrou foi, de um lado, que, com as novas tecnologias, era possível denunciar os abusos cometidos secretamente pelos Estados e, de outro lado, que as mídias tradicionais em geral não eram plenamente confiáveis, posto que representavam interesses dos anunciantes, à exceção de poucos veículos com linhas editorais ou jornalistas mais engajados em projetos contra-hegemônicos. O vídeo do ataque aéreo no Iraque impressionou o mundo pela indiferença e displicência dos soldados norte-americanos envolvidos na operação, que trataram a abordagem mais como um *game* do que como uma manobra militar. Tal fato recrudesceu o ódio aos EUA, que, por sua vez, recrudesceu seu temor de sofrer outros ataques ‘terroristas’, retroalimentando um cenário de pavor e paranoia,

traduzidos em aumento de formas de monitorar ‘inimigos’. Nessa conjuntura, misturando espionagem com ataques ‘cirúrgicos’ os EUA lançaram mão dos veículos aéreos não tripulados (VANT) – ou drones – com a dupla função de registrar imagens e matar pessoas.

Como afirma Fiori (2007), esta possibilidade de fazer guerras à distância e sem perdas humanas e o controle de uma moeda internacional sem padrão de referência que não seja o próprio poder do emissor mudaram radicalmente a forma de exercício do poder norte-americano sobre o mundo. Segundo ainda Fiori (2007), com a eliminação do poder de contestação soviético e com a ampliação do espaço desregulamentado da economia mundial de mercado, criou-se um novo tipo de território submetido às senhoriagens do dólar e à velocidade de intervenção das suas forças militares. Para Fiori (2007), logo depois da Segunda Guerra Mundial, a *Pax Americana* tinha um parentesco com os velhos impérios marítimos europeus na África e na Ásia, cuja estrutura de poder articulava-se por meio de redes militares, mercantis e financeiras apoiadas por fortalezas e feitorias, mas agora o novo poder monetário e balístico dos EUA lhes permitiu um maior distanciamento e o estabelecimento de uma forma de dominação que ainda mantém, em alguns casos, suas fortalezas, mas se desfaz, cada vez mais, das feitorias, substituídas pelo controle a distância dos bancos centrais das províncias incluídas dentro do seu território imperial; um território que dispensa fronteiras fiscais porque está recortado por fronteiras monetário-financeiras e estratégicas, facilitando a liderança do capital financeiro norte-americano, nos processos de fusões que promoveram, em todo o mundo, uma gigantesca centralização de capital durante os anos de 1980 e 1990. Fiori (2007) defende que o espaço desse novo tipo de império norte-americano não é contínuo nem homogêneo e que seu poder apoia-se no controle de estruturas transnacionais, militares, financeiras produtivas e ideológicas de alcance global, mas não suprime os Estados nacionais nem a hierarquia do sistema estatal. É por isso, portanto, que a prática da espionagem torna-se tão relevante.

No âmbito brasileiro, dois eventos são importantes para se compreender a relativa facilidade com que as espionagens denunciadas por Snowden foram executadas: 1) o contencioso Brasil x Estados Unidos da informática, nos anos 1980 (Ronald Reagan anunciou em 07 de setembro de 1985 um início de investigação sobre comércio desleal por parte do Brasil no campo da informática); e 2) a privatização das telecomunicações, nos anos 1990.

Segundo Vigevani (1995), a literatura tende a situar o momento inicial da informática no Brasil em 1968, quando convergiu para o Núcleo de Programas Especiais do Banco Nacional de Desenvolvimento o interesse da Marinha, representada pelo capitão-de-fragata Guaranys Rego, em desenvolver projetos que permitissem o domínio da tecnologia dos computadores que equipariam as fragatas em fase de aquisição e construção na Inglaterra. Em 1971, num simpósio

sobre política científica, discutiu-se amplamente o conceito de programa tecnológico e sua relação com a capacitação nacional. Em 1984 debateu-se ao longo do ano e aprovou-se em 3 de outubro o Projeto de Lei 10/84, que dispunha sobre a Política Nacional de Informática, cujo teor mais importante era a reserva de mercado à indústria brasileira. Embora ciente da repercussão, o Brasil, como afirma Vigevani (1995), não compreendeu bem todas as consequências internacionais da iniciativa e foi pego de surpresa com o discurso de Ronald Reagan, no qual se formulava oficialmente a possibilidade de retaliações econômicas por parte dos EUA contra o Brasil, caso não houvesse modificações na política brasileira de informática. A crise se oficializou em termos interestatais e diplomáticos em setembro de 1985, com a determinação de investigações contra o Brasil, sob a acusação de prática de formas desleais de comércio (*unfair trade*) contra os EUA, utilizando-se para esse objetivo a seção 301 do *Trade Act* de 1974.

Conforme defende Vigevani (1995), em um contexto em que, apesar da intensa e permanente presença do realismo, as análises globalistas tiveram notável incidência na formação na política norte-americana, bem como alimentaram, também fora dos EUA, os novos internacionalistas (no sentido liberal do termo), os elementos de interdependência nas relações internacionais, na medida em que cresceram cada vez mais, alteraram até qualitativamente o próprio conceito de soberania nacional, promovendo dessa forma novas estruturas de relações (os regimes internacionais), nos quais a ação dos Estados reduzir-se-ia e, numa visão grociana ou kantiana, prevaleceria definitivamente a capacidade de promover situações de vantagens multilaterais, eclipsando todas as concepções de 'jogos de soma zero'. O Brasil, não obstante a influência das teorias neoliberal e globalista, sofria uma crise de identidade da política exterior, o que enfraqueceu significativamente sua posição frente aos EUA. No caso da informática, o contencioso implicava questões de comércio, de investimentos e de direitos autorais, assim como cruzava, nas palavras de Vigevani (1995), o próprio tema da tecnologia e sua elaboração. Os EUA, em defesa dos interesses sobretudo do Estado, misturaram, em verdade, interesses estatais estratégicos e interesses de particulares (setor de informática): por um lado, os EUA queriam assegurar uma forte presença nacional nas indústrias emergentes de alta tecnologia e no crescimento dos setores no futuro; por outro, o Brasil, percebendo a importância do setor a longo prazo, desejava uma indústria de informática com capacidade de pesquisa e desenvolvimento nacionais.

Para Vigevani (1995), a questão da informática provocou um dos mais sérios e prolongados contenciosos nas relações do Brasil com os EUA e, como profetizou ele à época, poderia, segundo diferentes opiniões, passar à história como o símbolo do fim de uma

determinada fase e concepção de desenvolvimento econômico e social brasileiro, assim como da inserção internacional do Brasil. No contencioso, segundo Vigevani (1995), ao Brasil aplicaram-se as mesma regras e modalidades gerais, mas que acabaram atingindo alguns projetos nacionais de forma particular, como a intenção de desenvolver uma indústria de informática altamente tecnológica. E logrou-se o resultado a partir da clássica estratégia de acentuar o discurso liberal, internacionalista e as vantagens do livre comércio, mas contemplando uma realidade de medidas protecionistas, ainda que não declaradas. No final do segundo mandato de Reagan, em agosto de 1988, é aprovada nos EUA a Lei do Comércio, na qual assinalam-se formalmente as modificações havidas nos últimos dez anos, no contexto de uma economia global na qual o comércio, o desenvolvimento tecnológico, os investimentos e os serviços formam um sistema integrado em que cada parte afeta as outras e em particular a saúde da economia dos EUA.

Vigevani (1995) recorda que na América Latina a questão do progresso técnico esteve desde o final dos anos 1940 no foco das discussões políticas e de debates teóricos, os quais tiveram seus canais intelectuais e burocráticos de inserção no debate sobre a informática no Brasil. Nesse sentido, a mão invisível do mercado, nos termos colocados por Vigevani (1995), aparecia como madrasta: em vez de corrigir distorções, acentuava-as. A questão do progresso técnico esteve [e está], portanto, intimamente associada a uma determinada concepção de relações internacionais. Vigevani (1995) argumenta que, sendo assim, no Brasil, como em outros países, a indústria de informática não surgiria [como não surgiu] como consequência do fluir das forças produtivas ou da 'mão invisível' do mercado, mas como consequência de uma ação deliberada do Estado, de modo que os defensores da Política Nacional de Informática acreditavam que a informática, ao constituir um novo paradigma tecnológico, poderia, pela formação de uma massa crítica significativa que não pressupunha a existência completa dos outros estágios da civilização industrial, ser o ponto de partida para que o Brasil saísse do subdesenvolvimento. No entanto, apesar dos esforços, o Brasil não foi capaz de sustentar as posições iniciais, pelas dificuldades de consolidar uma política externa, econômica e industrial num contexto internacional conturbado e por outras razões que dizem respeito a um cenário interno marcado por instabilidade econômica, por crises debilitadoras do balanço de pagamentos, por pressões que acabaram pulverizando a indústria eletrônica, por não ter buscado associar-se ao setor financeiro e pela lenta aquisição de competitividade exportadora.

Quatorze anos depois da Política Nacional de Informática, um novo evento enterrou as chances de desenvolvimento nacional e amplo da indústria nacional brasileira de tecnologia de telecomunicações: a privatização do setor entre 1995 e 1998. Um dos motivos alegados para a

desestatização foi o de que o programa de privatização era uma possibilidade de contar com o aporte de recursos não inflacionários para financiar o déficit público. O Programa Nacional de Desestatização, conforme detalham Matos e Oliveira (1996), foi realizado em três etapas. Inicialmente, foi dada prioridade à alienação de empresas que haviam sido absorvidas pelo BNDES devido a problemas diversos. Em um segundo estágio, iniciado em 1991 com a privatização da Usiminas, foram privatizadas as empresas dos setores siderúrgico, petroquímico, de fertilizantes e do setor metal-mecânico e de aeronáutica, totalizando, até 1995, 38 empresas de grande porte, com uma receita estimada em US$ 9,122 bilhões. Posteriormente, foi conduzida a terceira e última etapa, consistindo na privatização dos serviços públicos.

Nas duas primeiras etapas, o governo privatizou cada uma das empresas por vez. Na terceira etapa, subdividiu as *holdings* setoriais (Eletrobrás, Telebrás), tentando evitar, assim, a ação de monopólios na economia. Cavalcante (2011) subdivide esta terceira etapa, a das telecomunicações, em outras três. A primeira é a decisão de quebra do monopólio e desestatização do setor desde início de 1995, com a aprovação de Emenda Constitucional e a elaboração do PASTE (Programa de Recuperação e Ampliação do Sistema de Telecomunicações e do Sistema Postal), buscando a valorização das companhias para a futura venda. A segunda etapa é inaugurada com a Lei Mínima de 1996, que possibilita e regulamenta exploração privada de serviços considerados não essenciais, como a telefonia celular. A terceira e derradeira fase vem com a aprovação da LGT (Lei Geral das Telecomunicações), que substitui o Código de 1962 exceto em relação à radiodifusão, e a concretização da venda do Sistema Telebrás em julho de 1998, após ser fatiado em quatro regiões, que agrupavam as antigas teles estaduais: três áreas de telefonia fixa local (assumidas por Telefônica, Telemar e Brasil Telecom) e uma de longa distância, a Embratel, todas essas operando em regime público de concessão.

Cavalcante (2011), fazendo referência a François Chesnais, recorda que as telecomunicações constituem, na atualidade, um setor fundamental das economias nacionais e do sistema produtivo mundializado, pois fornecem a base necessária sobre a qual se sustenta a circulação de informações para a acumulação de capital. No entanto, essas mesmas tecnologias podem ser dirigidas a finalidades distintas daquelas estabelecidas pelo mercado e seus usos coletivos podem escapar aos mecanismos de controle que buscam auferir ganhos às companhias do setor. Residiria aí, segundo Cavalcante (2011), uma contradição inerente ao desenvolvimento das telecomunicações, que incide sobre os programas do Estado e na sua relação com as empresas. Situação agravada pelo fato de que quando se faz referência a um "setor de telecomunicações", faz-se, na verdade, referência às diversas imbricações das formas

de comunicação tradicional, como a telefonia e o audiovisual, com os desenvolvimentos tecnológicos diversos da informática, que propiciaram novos ramos, como a internet, e que continuam a se proliferar com o auxílio de sistemas de informação baseados em *softwares* e na linguagem digital.

Estes dois eventos internos, mas igualmente conectados com o internacional, constituem no âmbito doméstico brasileiro os efeitos reais da política das grandes potências (EUA, no caso aqui estudado) e do modelo econômico então propagado por ela. No primeiro caso, o recuo brasileiro diante da reserva de mercado para a indústria de informática nacional inviabilizou controlar as fases de pesquisa e produção, por exemplo, de computadores de grande porte (*mainframe*), o que submete o país à dependência dos grandes centros, que exportam equipamentos com mecanismo de porta dos fundos, que, depois, funcionam como atalhos aos espiões das agências dos EUA, como denunciou Edward Snowden a Gleen Greenwald (2014). No segundo caso, a privatização de um setor estratégico como o das telecomunicações, especialmente no que diz respeito à internet, facilita as cooptações de agentes estrangeiros em relação a dados de particulares no Brasil (incluindo pessoas públicas), visto que de modo geral o único compromisso que as empresas têm é com o capital. O próximo item fará uma descrição por meio da qual se poderá observar a importância do domínio tecnológico para o desenvolvimento da contra-inteligência.

3. O PAPEL DA TECNOLOGIA, DO DEBATE ACADÊMICO E DA INSTITUCIONALIZAÇÃO E AS IMPLICAÇÕES PARA A SOBERANIA

Esta seção apresenta uma descrição sintética do desenvolvimento tecnológico de forma geral e sua consequência na transformação das técnicas de espionagem de forma particular, apontando o *continuum* do aprimoramento de ferramentas e meios que mediam a relação humana com a informação. Na sequência, reflete-se sobre o papel dos debates acadêmicos na institucionalização da espionagem como tema de pesquisa e a fragilidade das discussões no Brasil, o que reflete a própria condição nas quais estão postulados os serviços de inteligência nacionais, ainda voltados para ameaças internas. A seção é finalizada com uma abordagem sobre a quebra da soberania brasileira pela prática invasiva estadunidense.

3.1. TECNOLOGIA

Buzan (2012) menciona que quase tão óbvios como condutores dos estudos de segurança e defesa são os contínuo desenvolvimento de novas tecnologias e a necessidade de avaliar seus impactos nas ameaças, vulnerabilidades e estabilidades (ou não) das relações estratégicas. Recorda o autor que a chegada da bomba atômica em meados dos anos 1940 foi, por exemplo, praticamente o evento fundador dos Estudos Estratégicos e o impacto da tecnologia nuclear – e daquelas relacionadas a ela – durante a Guerra Fria mal pode ser exagerado, pois as armas nucleares forneciam grande capacidade adicional de poder destrutivo pela primeira vez na história militar. Lembra ainda que os mísseis balísticos de longo alcance diminuíram o tempo de resposta e eram capazes de carregar ogivas nucleares, um desenvolvimento tecnológico que livrou as armas nucleares dos vulneráveis sistemas de lançamento de bombardeios, aumentando enormemente a capacidade de lançar um primeiro ataque contra o oponente. Adverte também Buzan (2012) que a tecnologia não precisa ser exclusivamente do tipo militar para ter impacto na segurança e defesa, até por que a história das tecnologias militares e civis geralmente é de interação e ‘dupla utilização’, como, por exemplo,

a internet, que foi primeiramente desenvolvida como uma tecnologia militar e como uma rede distribuída para transferir informações sob um ataque nuclear. Assim, para Buzan (2012), mesmo que a tecnologia não seja o principal condutor no desenvolvimento da segurança e defesa, ela é, sem dúvida determinante em primeiro lugar porque a própria tecnologia é influenciada pelas outras forças motrizes e em segundo porque há agentes humanos (civis, militares, comerciais e públicos) que tomam decisões sobre quais tecnologias desenvolver.

Em termos de desenvolvimento técnico, classicamente faz-se referência a três grandes revoluções: 1ª Revolução Industrial (iniciada na Inglaterra, no século XVIII (1780-1830); 2ª Revolução Industrial (iniciada por volta de 1870, mas consolidada nas primeiras décadas do século XX, como um fenômeno muito mais dos Estados Unidos que dos países europeus); e 3ª Revolução Industrial – ou Revolução Tecnológica (iniciada na década de 1970, tendo por base a alta tecnologia ou tecnologia de ponta - "*high tech*"). O ramo característico da Primeira Revolução Industrial foi o têxtil de algodão, aparecendo ao seu lado a siderurgia, dada a importância que o aço teve na instalação de um período técnico apoiado na mecanização do trabalho; consequentemente, a tecnologia característica foi a máquina de fiar ou o tear mecânico, sendo todas as máquinas movidas a vapor originado da combustão do carvão, que também alimentava o sistema de transporte característico: a ferrovia e a navegação marítima.

Hobsbawm (1996) lembra que foi no período do auge das revoluções industriais, justamente entre 1848 e 1870, que o mundo se tornou capitalista e uma minoria significativa de países 'desenvolvidos' transformou-se em economias industriais, fazendo, por exemplo, as exportações inglesas nos primeiros sete anos da década de 1850 crescerem sem comparação a períodos anteriores, além disso, se entre 1820 e 1850 as exportações de produtos de algodão inglês cresceram em 1.100 milhões de jardas, entre 1850 e 1860 elas cresceriam mais de 1.300 milhões. Segundo Hobsbawm (1996), o número de máquinas de algodão cresceu de 100 mil entre 1819 e 1821 e 1844 a 1846 para o dobro disso na década de 1850. A expansão econômica durante a Primeira Revolução Industrial, para Hobsbawm (1996), é mais convenientemente medida em estatísticas: entre 1850 e 1870, a produção mundial de carvão multiplicou-se por duas vezes e meia, a produção de ferro multiplicou-se por quatro vezes; a força do vapor multiplicou-se por quatro vezes e meia, subindo de uma estimativa de 4 milhões de HP em 1850 para cerca de 18,5 milhões de HP em 1870.

Vários avanços revolucionários da tecnologia já estavam, conforme Hobsbawm (1998), em gestação ou nascendo à época de transição da Primeira para a Segunda Revolução Industrial: os vários tipos de turbinas e motores de combustão interna, o telefone, o gramofone e a lâmpada elétrica incandescente (todos sendo inventados), o automóvel, que Daimler e Benz tornaram

operacional nos anos 1880, sem falar do cinematógrafo, da aeronáutica e da radiotelegrafia, produzidos ou pesquisados nos anos de 1890

A Segunda Revolução Industrial esteve por trás de todo desenvolvimento técnico, científico e de trabalho que ocorreu nos anos da Primeira e, principalmente, da Segunda Guerras Mundiais. Tendo suas bases nos ramos metalúrgico e químico, a Segunda Revolução Industrial caracterizou-se pelo aço, que se tornou um material tão básico que foi nele que a siderurgia ganhou sua grande expressão. O período foi marcado ainda pela indústria automobilística, que criou o sistema de técnica e de trabalho conhecido como fordista, caracterizado pelo paradigma de regulação técnica e da produção padronizada. Além do aço e da metalurgia, a tecnologia característica desse período foi também a eletricidade, a eletromecânica, o petróleo, o motor a explosão e a petroquímica, sendo a eletricidade e o petróleo as principais formas de energia.

A Terceira Revolução Industrial caracterizou-se pelas atividades mais criativas, que exigiam elevada qualificação da mão-de-obra e tinham horário flexível. Tem no toyotismo sua marca principal: abolir a função de trabalhadores profissionais especializados para torná-los especialistas multifuncionais, lidando com as emergências locais anonimamente. A tecnologia característica desse período, que tem início no Japão, é a microeletrônica, a informática, a máquina CNC (Controle Numérico Computadorizado), o robô, o sistema integrado à telemática (telecomunicações informatizadas) e a biotecnologia. Sua base mistura a Física e a Química, a Engenharia Genética e a Biologia Molecular, sendo o computador a máquina da terceira revolução industrial. As novas regiões industriais de alta tecnologia de ponta unem centros produtores de tecnologia com indústrias de informações, associados a grandes centros de pesquisa (universidades): os tecnopólos, sendo o principal o Vale do Silício.

O impacto do imperativo tecnológico na prática da espionagem foi decisivo na facilitação dos muitos meios que a engenhosidade humana buscou – e tem buscado - para superar o maior obstáculo de um espião: o ato de conseguir qualquer informação de inteligência sem ser capturado. No caso, por exemplo, da criptografia, que foi utilizada pela primeira vez no antigo Egito e na Mesopotâmia, houve um avanço fenomenal durante a Primeira e Segunda Guerras Mundiais, quando a capacidade de decodificar informações sobre os movimentos do inimigo desempenhou um papel fundamental[10].

Na década de 1970, conforme Harding (2014), *softwares* de criptografia como o Pretty

[10] O telegrama Zimmerman é ilustrativo: durante a I Guerra Mundial o telegrama foi interceptado pela organização criptológica da marinha real britânica (*Room* 40), no qual a Alemanha propunha ao México que atacasse os EUA em troca da reconquista dos territórios perdidos na guerra de 1844 caso a Alemanha vencesse a guerra. A revelação do conteúdo do telegrama foi um dos fatos que levou os EUA a entrarem na guerra do lado dos britânicos e franceses. (Cepik, 2001)

Good Privacy (ou simplesmente PGP) estavam disponíveis para uso particular, bem como por organizações comerciais. A criptografia passou então a ser um desafio primário para agências de inteligência ocidentais, ansiosas para continuar a ler mensagens de seus adversários. Harding (2014) lembra que a administração Clinton respondeu tentando inserir *backdoor* (porta dos fundos) em sistemas de criptografia comerciais, o que permitiria acesso da NSA a computadores fora dos EUA. Embora a iniciativa tenha sido derrotada no Congresso dos EUA, a prática, como revelou Edward Snowden, ocorre com frequência ainda hoje. Segundo Harding (2014), em 2000, com a criptografia sendo cada vez mais empregada por prestadores de serviços e indivíduos em suas comunicações *on-line* cotidianas, a NSA gastava bilhões de dólares tentando encontrar maneiras de contorná-la, buscando na rede mundial de computadores *chats*, *e-mails,* dados pessoais, telefonemas e até mesmo registros bancários e médicos. Para Harding (2014), teria sido apenas em 2010 que a NSA conseguiu um progresso considerável, graças ao uso de supercomputadores para quebrar algoritmos, os blocos básicos de criptografia[11].

Para Cepik (2001), diferentemente das áreas de *humint (human intelligence), imint (imagery intelligence) e sigint (signals intelligence),* nas quais haveria certas características intrínsecas da informação coletada que organizam a disciplina (relatos, imagens e códigos decifrados), nas áreas de *masint* (*measurement and signature intelligence*) e vigilância espacial há uma grande diversidade de tipos de dados coletados e empregos desses mesmos dados, tornando a identidade da disciplina mais frouxa a despeito de sua importância crescente. Não seria à toa, então, para Cepik (2001), que nas áreas de *imint* (remonta ao começo do século XX) e *masint* (remonta ao início dos anos 1980) é que o desenvolvimento tecnológico é mais perceptível: no primeiro caso, a chamada inteligência de imagens (ou *imint*) passou a ser obtida principalmente a partir de plataformas aerotransportadas e espaciais, com imagens fotográficas analógica e digitais de resolução cada vez maior, além de também poder ser coletada e produzida utilizando-se sensores especiais para outras porções do espectro eletromagnético invisíveis ao olho humano (próximas de infravermelho, termais, radar[12]), e ainda a partir de sensores multiespectrais e hiperespectrais, capazes de produzir imagens através de bandas eletromagnéticas diversas que permitem detectar forma, densidade, temperatura, movimento e composição química dos objetos; no segundo caso, a chamada inteligência de mensuração e assinatura (ou *masint*) passou a ser obtida a partir de características singulares – as assinaturas

[11] Talvez a consequência mais inesperada do caso Snowden tenha sido o retorno da máquina de escrever: os governos indiano e russo, a partir do verão de 2013, suspenderam o armazenamento em formato eletrônico de tudo que fosse ultrassecreto. (Harding, 2014).

[12] Autores como P.B. Stares (1991) e F.H. Hinsley (1993) consideram o radar a mais importante e revolucionária inovação na área de informações durante a II Guerra Mundial (Cepik, 2001).

– de sistemas de armas, aeronaves, embarcações e radares, além de monitorar dados geofísicos (acústicos, sísmicos e magnéticos), radiações nucleares, composição físico-química de materiais e uma variedade de fontes para a montagem de bancos de dados, análise e posterior emprego tático, estratégico e diplomático (também são empregados pelas potências com programas aeroespaciais mais desenvolvidos em sistemas terrestres e espaciais para vigilância das atividades aeroespaciais de outros países).

Nesse sentido, as revoluções industriais, por expandirem as formas de comunicação, tornaram a tarefa da espionagem menos árdua, ainda que todo método já inventado, como aponta Volkman (2013), por mais inteligente que seja, sempre carrega defeitos, sendo o mais perigoso a autoincriminação. Volkman (2013) relembra que desde a China antiga, quando mandarins raspavam a cabeça de um espião, escreviam uma mensagem secreta no crânio calvo dele, esperavam até que o cabelo crescesse de novo, e enviavam o espião para sua missão; passando pelos gregos (480 a.C), que conceberam um método que envolvia a escrita numa folha de papiro, no sentido do comprimento, enrolada em torno de um bastão, sendo inteligível, quando removida e enviada, apenas para um destinatário que tinha um bastão idêntico, precisamente de mesmo diâmetro e comprimento; passando ainda pelos tempos medievais, quando se estimulou o desenvolvimento da escrita invisível nas missivas (a técnica utilizava certos líquidos incolores – mais popularmente suco de limão ou sulfato de cobre - que se tornavam visíveis pela aplicação de calor ou de produtos químicos); e chegando até ao início do século XX, no desenvolvimento do rádio, que prometia uma revolução nas comunicações de espionagem, visto que os espiões podiam transmitir sua inteligência em longas distâncias de dentro de um país inimigo, ou ainda na tecnologia fotográfica, que proporcionou novos dispositivos para mensagens de espionagem, ou no microponto alemão da 2ª Guerra Mundial, que reduzia fotografias ao tamanho de um pequeno ponto que podia ser escondido atrás de um selo postal ou no meio de uma frase de uma carta, ou ainda, durante a Guerra Fria, no transmissor a explosão da CIA, que consistia em um pequeno rádio que comprimia eletronicamente até mesmo uma mensagem muito longa em um ponto eletrônico minúsculo, ou, atualmente, na inovação que esconde mensagens em imagens digitais no computador, muito semelhante a proteções de direitos autorais criptografados, escondidos em alguns programas de *software* e DVDs; toda essa engenhosidade, desde a China antiga até hoje, não conseguiu, para Volkman (2013), criar nenhum método infalível de comunicação da espionagem, uma vez que, mesmo a tecnologia mais brilhante requer um espião para estar de posse dela, o que é, portanto,

prova de acusação de espionagem. Por isso mesmo, Woloszyn [13] acredita que o grande diferencial para a comunidade de Inteligência do século XXI está no preparo técnico-profissional e na mudança de mentalidade de seu pessoal (agentes de campo, analistas e gestores) acrescido do uso de novas tecnologias, que tornaram as escutas em massa algo muito mais viável.

Não somente as escutas em massa, mas, no século XXI, a comunicação e a informação conectariam os seres humanos de forma massiva e jamais vista, de modo que especialmente após os anos 2000, as tecnologias de informação iriam influenciar drasticamente não só as práticas estatais de espionagem, como também as ações ocultas de indivíduos conectados em rede, por meio da internet, numa dialética infinita de retroalimentação. Cepik et al. (2014) notam que o crescimento atual da Internet é marcado por duas tendências atualmente: *ubiquidade* e *convergência digital*. Para os autores (2014), a *ubiquidade* diz respeito à qualidade de onipresença da rede, com dispositivos de todo o tipo sendo desenvolvidos para conectarem-se uns aos outros, utilizando os protocolos de comunicação da Internet; já a *convergência digital* seria um fenômeno social complexo de integração de mídias distintas em um único canal de transmissão, a qual vem revolucionando as instituições e o modo de produção midiática do século XX. Um moderno telefone celular, por exemplo, seria, ao mesmo tempo, uma televisão, um rádio, um telefone, um *modem*, uma máquina fotográfica, e, ainda, uma plataforma de acesso à *web*[14]. Por isso, Castells (2005) defende que a sociedade contemporânea deixou de ser industrial e se afirma cada vez mais informacional, não sendo o conhecimento e a informação centrais na atual sociedade (posto que eles sempre o foram, em todas as sociedades historicamente conhecidas), mas sendo novo o fato de serem de base microeletrônica, através de redes tecnológicas que fornecem novas capacidades a uma velha forma de organização social: as redes.

Nesse sentido, para Castells (2005), embora a tecnologia seja condição necessária, não é suficiente para a emergência de uma nova forma de organização social baseada em redes, ou seja, na difusão de redes em todos os aspectos da atividade na base das redes de comunicação digital. Nesse caso, o desenvolvimento da tecnologia ajudaria só quando fosse combinado com

---

13 Revista Diálogo, Volume 22, N.4 André Luís Woloszyn é Tenente-Coronel do Exército Brasileiro.

14 Durante o encontro entre Edward Snowden e Gleen Greenwald, em Hong Kong, ocasião em que ocorreu a delação, Greenwald (2014) relata: “Ele [Snowden] foi logo falando em segurança e perguntou se eu tinha um telefone celular. Meu telefone só funcionava no Brasil, mas mesmo assim ele insistiu que eu tirasse a bateria ou pusesse o aparelho dentro do congelador do minibar, o que pelo menos abafaria a conversa e a tornaria mais difícil de interceptar”. O relato é icônico da *convergência digital* referida por Cepik et at.(2014).

mudanças nas estruturas de base, pois a comunicação em rede transcende fronteiras, a sociedade em rede é global e baseada em redes globais. Então, a sua lógica chegaria a países de todo o planeta e difundir-se-ia através do poder integrado nas redes globais de capital, bens, serviços, comunicação, informação, ciência e tecnologia. Para Castells (2005), aquilo a que chamamos globalização é outra maneira de nos referirmos à sociedade em rede, ainda que de forma mais descritiva e menos analítica do que o conceito de sociedade em rede implica, porém, como as redes são seletivas de acordo com os seus programas específicos, e porque conseguem, simultaneamente, comunicar e não comunicar, a sociedade em rede difunde-se por todo o mundo, mas não inclui todas as pessoas, excluindo, neste início de século, a maior parte da humanidade, embora toda a humanidade seja afetada pela sua lógica, e pelas relações de poder que interagem nas redes globais da organização social.

É nesta sociedade em rede, definida por Castells (2005) como 'uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microeletrônica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes' que cresceu Edward Snowden[15], um norte-americano nascido na Carolina do Norte e criado em Maryland, em uma família de classe média baixa de funcionários públicos federais (seu pai trabalhara por trinta anos na Guarda Costeira).

Segundo Greenwald (2014), na adolescência, Snowden se sentia muito pouco desafiado no ensino médio, que nunca chegara a concluir, interessando-se muito mais pela internet do que pelas aulas. Harding (2014) acrescenta que ele jogava Tekken [jogo eletrônico] obsessivamente; encarar a batalha de todo homem lutando contra o mal, contra as probabilidades, moldou sua visão moral, disse mais tarde. Entre 2002 e 2004, trabalhou como *webmaster* para a Ryuhana Press, um *website* japonês de animação.

Após o 11 de setembro, Snowden tornou-se um 'patriota' e, em 2004, alistou-se no exército com o objetivo de combater na Guerra do Iraque, que na época considerava um esforço nobre para libertar o povo iraquiano da opressão (após poucas semanas no treinamento básico, viu que se falava muito mais em matar árabes do que em libertar quem quer que fosse; saiu desiludido da corporação depois de quebrar as duas pernas em um treinamento). Embora tivesse largado o ensino médio, tinha uma facilidade inata para a tecnologia, o que lhe garantiu o emprego de segurança digital no Centro de Estudos Avançados em Linguagem da Universidade

[15] Todas as informações sobre a biografia de Edward Snowden foram retiradas de Greenwald (2014) e Harding (2014).

de Maryland, edifício secretamente administrado e usado pela NSA[16]. Logo trocou o cargo de segurança pelo de especialista em tecnologia na CIA, em 2005. Em 2006 deixou de ser prestador de serviços para a CIA e entrou para o quadro de funcionários. Em 2007 foi trabalhar na Suíça, onde ficou até 2009, operando em segredo, com credenciais diplomáticas.

No final de 2009, novamente desiludido, Snowden decidiu sair da CIA e começou a pensar em se tornar delator e em vazar segredos que acreditava revelarem comportamentos questionáveis. Muda para o Japão, dessa vez como terceirizado da Dell Corporation, que prestava serviços à NSA, período em que teria aprendido a ser *hacker* e teria passado a dominar os mais sofisticados métodos para proteger dados eletrônicos da intrusão de outras agências de segurança, recebendo certificação formal como agente cibernético de alto nível, do tipo capaz de *hackear* sistemas civis e militares de outros países para roubar informações ou preparar ataques sem deixar vestígios. Ao fim de sua temporada com a NSA no Japão, em 2011, Snowden foi trabalhar em um escritório da CIA, no estado de Maryland, outra vez como terceirizado da Dell, indo daí para o Havaí, em 2012.

No início de 2013, percebeu que havia ainda mais um conjunto de documentos de que precisava para completar o retrato que desejava mostrar ao mundo com suas delações, mas que, segundo Greenwald (2014), não poderia acessar enquanto estivesse na Dell. Só poderia colocar as mãos neles se conseguisse outro cargo no qual fosse formalmente nomeado analista de infraestrutura, o que lhe daria alcance ilimitado aos repositórios de vigilância gerais da NSA. Com esse objetivo, candidatou-se a uma vaga no Havaí, na Booz Allen Hamilton, uma das maiores e mais poderosas prestadoras de serviços na área de defesa dos EUA, em que trabalham ex-altos funcionários do governo, o que lhe permitiu coletar informações sobre o monitoramento secreto realizado pela NSA de toda a infraestrutura doméstica de telecomunicações dos EUA. Em meados de maio de 2013, solicitou algumas semanas de licença para tratar sua epilepsia, doença da qual descobrira ser portador um ano antes.

Depois de um enredo cinematográfico, envolvendo conversas cifradas pela internet, saída dos EUA e desembarque na China, chegou a Hong Kong no dia 20 de maio de 2013, quando e onde revelou ao Gleen Greenwald (jornalista do The Guardian) o que sabia, não explicando por completo, entretanto, segundo Harding (2014), como realizou o vazamento, embora, como administrador de sistemas, fosse conhecido seu livre acesso à NSAnet, o sistema

[16] Agência Nacional de Inteligência dos EUA. Organismo central das 16 agências de inteligência estadunidense. Braço do Pentágono, a NSA é a maior agência de inteligência do mundo, e grande parte de seu trabalho de vigilância é conduzida pela aliança dos Cinco Olhos (EUA, Canadá, Austrália, Nova Zelândia e Inglaterra). (Harding (2014); Greenwald (2014)).

de intranet da NSA, criado logo depois do 11 de setembro, para melhorar a conexão entre as diferentes partes da comunidade de inteligência dos EUA. Snowden considera seu vazamento não como uma atitude de traição, mas como um corretivo necessário para um sistema de espionagem que se tornou disfuncional, segundo ele.

Curiosamente, Snowden preferiu fazer suas revelações não pelo WikiLeaks - de quem tinha sofrido forte influência e com quem mantinha vínculos por meio da amizade com Julian Assange -, mas por meio de um jornalista (Gleen Greenwald) do jornal The Guardian, sob a alegação de que se quisesse os documentos simplesmente postos na internet todos de uma vez, poderia ter feito ele mesmo, desejando, na verdade, que as matérias fossem escritas, uma a uma, de forma que as pessoas pudessem entender o que acontecia de fato, além do que, possivelmente o mais importante, como aponta Harding (2014), o *website* do WikiLeaks estava fora do ar e Assange estava sob vigilância, preso numa embaixada estrangeira.

Para Harding (2014), muito antes da história de Snowden tornar Greenwald conhecido, o jornalista já tinha acumulado seguidores: litigante por profissão, ele passou uma década trabalhando nas cortes federal e estadual; filho de judeus, truculento, homossexual, radical e fervoroso quanto à liberdade civil, Greenwald encontrou voz na era Bush, abrindo mão, em 2005, de advogar para se concentrar na escrita em tempo integral de seu *blog*, que atraiu – e atrai - uma legião de leitores. Harding (2014) aponta ainda que Greenwald foi um crítico irascível das administrações Bush e Obama. Fez críticas mordazes aos 'recordes' de Washington, colocando em sua agenda os direitos dos cidadãos, os ataques por mísseis guiados, as guerras estrangeiras, o engajamento desastroso dos EUA no mundo muçulmano, a baía de Guantánamo, o regime norte-americano de tortura mundial. A visão franca de Greenwald sobre privacidade sem dúvida o tornaram, para Harding (2014), o mais conhecido crítico da vigilância do governo, atraindo as atenções de Snowden.

Conforme Harding (2014), Snowden refletiu durante meses sobre o planejamento de seu acordo com a mídia, sendo minucioso ao condicionar a entrega do material aos alvos dessa vigilância, de modo que a mídia de Hong Kong deveria ter a informação relativa à espionagem a Hong Kong, o material brasileiro deveria ir à mídia brasileira e assim por diante. Alegou que se o material caísse em mãos de terceiros, adversários como russos ou chineses, isso o deixaria aberto às acusações de que não passava de um desertor, ou agente estrangeiro, algo que não considerava verdade. O jornal *The Guardian* teria sido escolhido como veículo para tornar públicas suas denúncias, então, pelo fato de ter um histórico de quebras e rompimento das regras implícitas do jornalismo tradicional, criadas para diminuir o impacto das revelações e proteger o governo.

A partir daí iniciaram-se as revelações pelo jornal *The Guardian* em quatro matérias distintas:

1) sobre a ordem secreta da FISA (Lei de Vigilância de Inteligência Estrangeira de 1978) que obrigava a Verizon, um dos maiores provedores de telefonia norte-americanos, a ceder à NSA todos os registros de todos os cidadãos dos EUA;
2) sobre o programa de grampos não autorizados da era Bush;
3) sobre o programa BOUNDLESS INFORMANT, de rastreamento de dados da NSA por meio de coleta, análise e armazenamento de bilhões de chamadas telefônicas e e-mails obtidos da estrutura norte-americana de telecomunicações;
4) sobre o programa PRISM, que permitia à NSA obter praticamente o que quisesse das empresas de internet (Google, Apple e Facebook) que centenas de milhões de pessoas no mundo agora usavam como principal meio de comunicação.

Neste último caso, embora as empresas de internet negassem o conhecimento do programa PRISM, Harding (2014) lembra que em reportagem do jornal Washington Post, intitulada "Inteligência dos EUA e da Grã-Bretanha coleta dados de nove empresas norte-americanas de internet em amplo programa secreto", afirmou-se que a NSA e o FBI estavam acessando diretamente os servidores centrais de nove das maiores empresas de internet dos EUA para obter dados de áudio e vídeo, fotos, *e-mails*, arquivos e *logs* de conexão que permitiam aos analistas rastrear alvos estrangeiros. Tudo, segundo o jornal, com participação consciente das nove empresas nas operações do programa PRISM: Microsoft [supostamente a primeira a oferecer material ao PRISM, em 11.09.2007], Yahoo! [março de 2008], Google [janeiro de 2009], Facebook [junho de 2009], PalTalk [dezembro de 2009], AOL [março de 2011], Skype [data não sabida], YouTube [data não sabida] e Apple [outubro de 2012, exatamente um ano após a morte de Steve Jobs]. Em uma das imagens vazadas, reproduzida no Brasil pelo jornal O Globo (figura 1), vê-se por meio de um *slide* de apresentação sobre o programa PRISM que, através de Facebook, Gmail, Youtube, Yahoo, Hotmail, Google e Skype, a NSA levantou informações sobre o petróleo na Venezuela, energia no México e tráfico na Colômbia:

Figura 1: *Slide* de apresentação sobre o programa PRISM

Fonte: Jornal *O Globo* (http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/)

Lê-se, de cima para baixo, da esquerda para a direita: "Uma semana na vida de relatórios PRISM / Amostragem de relatórios tópicos de 2 a 8 de fevereiro de 2013 / Venezuela / Aquisição de material militar / Petróleo / México / Narcóticos / Energia / Segurança Internacional / Assuntos Políticos / Colômbia / Tráfico / FARC" (tradução própria).

Os documentos surpreendiam pelas datas recentes: 2011 e 2012 na maioria, 2013 em muitos casos, alguns chegavam a ter datas de março e abril de 2013, poucos meses antes da delação. Entretanto, segundo Harding (2014), o conjunto era de difícil manuseio, pois alguns documentos eram "obviamente delicados", mas a maioria era confusa e corporativa: *PowerPoints*, *slides* de treinamento, relatórios gerenciais e diagramas de programas de extração de dados.

Segundo Greenwald (2014), dos milhares de programas de vigilância distintos descritos pelo acervo de Snowden, muitos tinham por alvo a população dos EUA, mas dezenas de países mundo afora – inclusive democracias em geral vistas como aliadas dos EUA, como França, Brasil, Índia e Alemanha – também foram alvo de uma vigilância em massa indiscriminada. Grande parte dos documentos do acervo de Snowden, conforme Greenwald (2014), tinha a classificação *top secret*[17], "ultrassecreto", sendo a maioria assinalada pelo acrônimo "FVEY",

[17] As classificações de segurança são feitas através da atribuição de marcadores externos que definem a importância de cada informação para a segurança nacional (tipicamente, são utilizadas as categorias de confidencial, secreto e ultrassecreto). A atribuição da categoria de ultrassecreto só pode ser feita pela autoridade mais alta do país ou por sua expressa delegação. (Cepik, 2001b) No caso do sistema

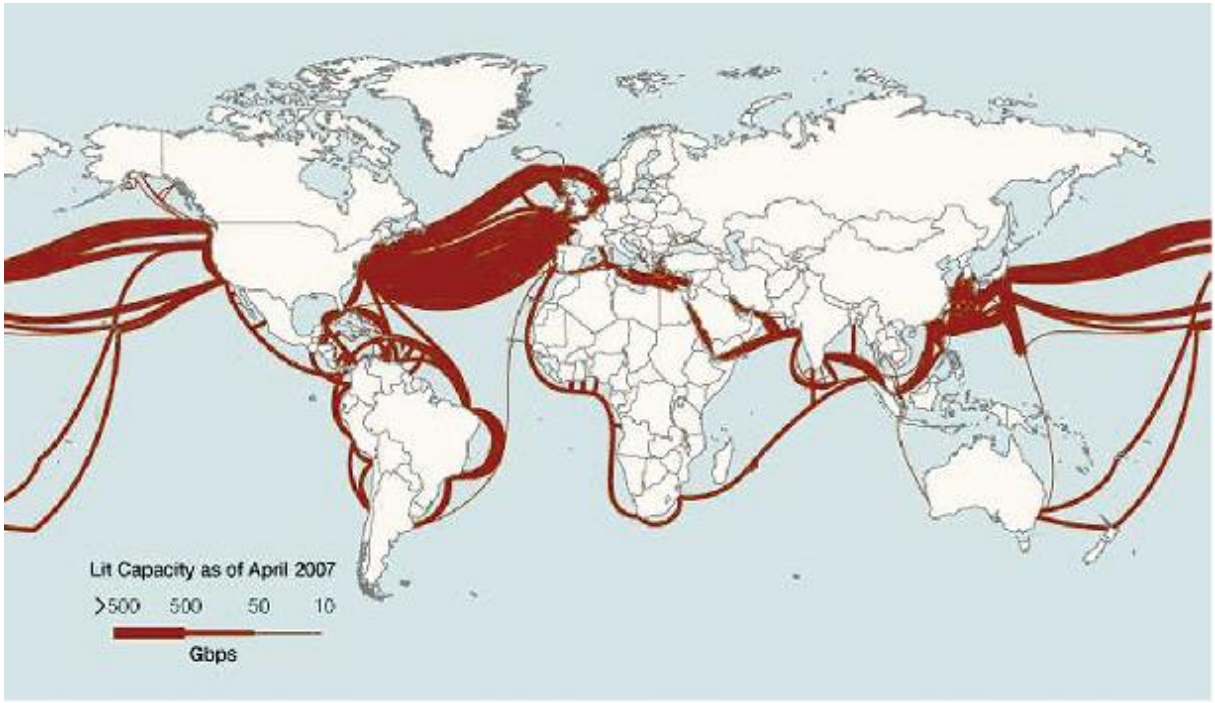
ou seja, só tinha aprovação para circular entre os quatro aliados de vigilância mais próximos da NSA, a aliança dos Cinco Olhos (*Five Eyes*), formada com países de língua inglesa.

O acervo revelava os recursos técnicos usados para interceptar comunicações: o monitoramento, pela NSA, de servidores de internet, satélites, cabos de fibra óptica submarinos [18], sistemas de telefonia nacionais e estrangeiros e computadores pessoais. Especialmente no que diz respeito aos cabos submarinos, as principais rotas de tráfego de dados pelo oceano saem da região de Nova York com destino à Europa, majoritariamente com conexões na França e no Reino Unido. Outro conjunto grande de cabos é encontrado ao longo da costa Oeste americana e ligando a Califórnia com *backbones* (suporte principal) em diversos pontos da extrema Ásia, como Japão, Sudeste da China e ilhas do Pacífico. O Brasil possui suas principais conexões com a Argentina e, para acessar dados de servidores na Europa ou Estados Unidos, os cabos que partem do Brasil quase todos passam pelo Caribe. Há uma única rede ligando o Brasil à África, tratando-se de um conjunto de cabos que sai da região do Rio Grande do Norte até as ilhas de Cabo Verde e, de lá, até o Senegal. O mapa a seguir (figura 2) mostra a quantidade de dados transmitidos por fibra ótica, através de cabos submarinos, que a NSA podia capturar em abril de 2007:

Figura 2: Quantidade de dados transmitidos por fibra ótica através de cabos submarinos

de classificação dos Estados Unidos, por exemplo, além das três categorias ascendentes de segurança (*confidential*, *secret* e *top secret*), são utilizados cerca de cinquenta marcadores adicionais que, embora não tenham o mesmo estatuto legal, muitas vezes estabelecem regulação mais intensa do que o sistema formal. (Cepik, 2001a)

[18] 95% das comunicações mundiais são feitas por cabo submarinos (International Cable Protection Committee). Qualquer defesa que necessite de rede para agir é inútil se o acesso a ela for negado.



Fonte: Jornal *O Globo* (http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/)

Havia a identificação de indivíduos escolhidos para serem alvos de formas de espionagem invasivas ao extremo, lista que ia de supostos terroristas e suspeitos de crimes a líderes democraticamente eleitos de aliados dos EUA e até mesmo cidadãos norte-americanos comuns. Harding (2014) recorda que os pontos de desembarque dos cabos submarinos, por exemplo, são tão importantes que o Departamento de Segurança Interna norte-americano os considera como infraestrutura nacional crítica (de acordo com mensagens diplomáticas dos EUA vazadas), de modo que no novo mundo das comunicações regidas pela internet, a posição da Grã-Bretanha na ponta oriental do Atlântico a torna um eixo central, já que aproximadamente 25% do tráfego mundial da internet hoje atravessa o território britânico por esses cabos, no caminho entre os EUA e a Europa, África e todos os pontos do Oriente. A maior parte do tráfego restante de informações parte ou chega a pontos dentro dos EUA, tornando os dois países os maiores hospedeiros dos crescentes fluxos de dados do planeta. No período, por exemplo, de um mês (a partir de 8 de março de 2013), o programa BOUNDLESS INFORMANT mostrava que uma única unidade da NSA, chamada *Global Access Operations* (Operações de Acesso Global, GAO na sigla em inglês), tinha coletado dados sobre mais de 3 bilhões de chamadas telefônicas e *e-mails* que haviam transmitido pelo sistema de telecomunicações norte-americano (o Twitter teria se negado a facilitar as coisas para o governo, outras companhias, no entanto, teriam se mostrado mais cooperativas, como mencionado anteriormente).

Conforme Greenwald (2014), no geral, em apenas trinta dias, a unidade coletou dados sobre mais de 97 bilhões de *e-mails* e 124 bilhões de chamadas do mundo inteiro (no Brasil, foram 2,3 bilhões). Para coletar uma quantidade tão avassaladora de comunicações, a NSA dependeu – e depende - de inúmeros métodos, entre eles a interceptação direta dos cabos de fibra óptica (inclusive os marítimos) usados para transmitir comunicações internacionais, o redirecionamento das mensagens para repositórios da NSA quando estas atravessam o sistema dos EUA (como é o caso da maioria das comunicações no mundo) e a cooperação com serviços de inteligência de outros países. Com frequência cada vez maior, a agência também conta com as empresas de internet e de telefonia, que repassam as informações coletadas de seus próprios clientes (a NSA tem em torno de 30 mil funcionários, mas mantém contrato com cerca de 60 mil funcionários de companhias particulares). A parceria entre a NSA e as empresas de telecomunicações é altamente lucrativa, já que, segundo Harding (2014), em troca do acesso a 81 por cento das chamadas telefônicas internacionais, Washington paga às gigantes das telecomunicações muitas centenas de milhões de dólares por ano.

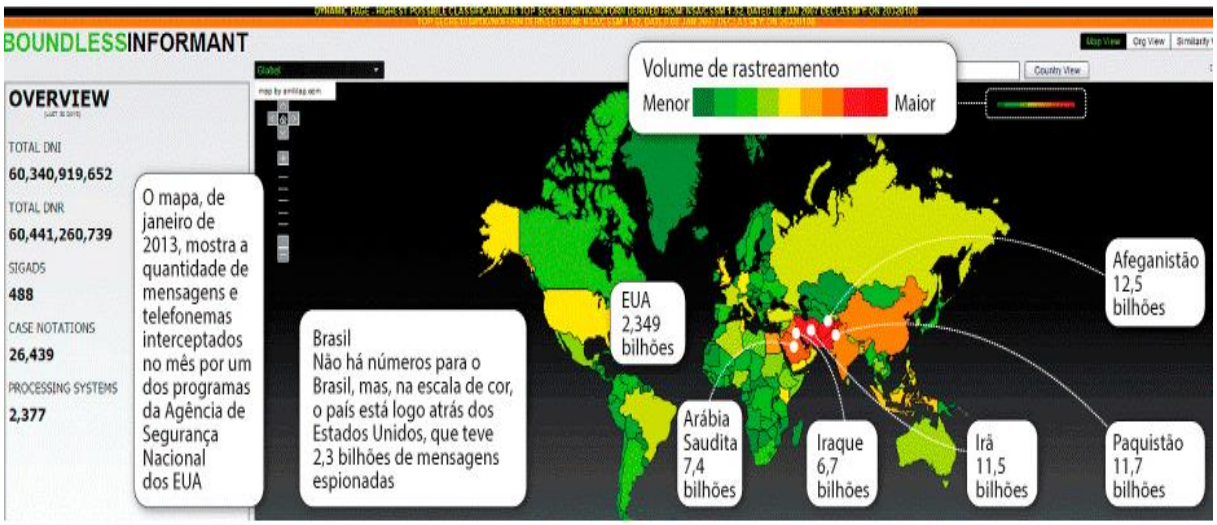
De modo geral, a NSA tem três categorias diferentes, segundo Greenwald (2014), de relações com os países estrangeiros: a) com o grupo dos Cinco Olhos[19], em que os EUA espionam junto com tais países, mas raramente os espionam, a menos que solicitados pelas autoridades dos próprios países parceiros; b) com os países com os quais a NSA trabalha em projetos de vigilância específicos ao mesmo tempo que os espiona de forma ampla; e c) com os países que os EUA espionam de forma rotineira, mas com os quais quase nunca cooperam.

O Brasil, considerado uma incógnita aos EUA (aparece como "amigo, inimigo ou problema?" em documento secreto), enquadra-se na categoria "c", tendo sido alvo constante da espionagem estadunidense: além do programa BOUNDLESS INFORMANT, também esteve na mira do programa canadense OLYMPIA, destinado a vigiar o Ministério das Minas e Energia brasileiro; do programa BLARNEY, que explora o acesso de determinadas empresas de telecomunicações a sistemas internacionais depois de elas terem firmado contratos com companhias semelhantes no exterior para criação, suporte e melhoria de suas redes; do programa OAKSTAR, que explora de maneira semelhante ao BLARNEY o acesso de um dos 'parceiros' corporativos da NSA a sistemas de telecomunicações estrangeiros, e usa esse acesso para redirecionar dados para os repositórios da agência (tanto a NSA quanto as empresas

[19] (National Security Agency (NSA) dos Estados Unidos, Government Communications Headquarters (GCHQ) do Reino Unido; Serviço de Segurança de Comunicações Canadense (CSEC) do Canadá; Australian Signals Directorate (ASD) da Austrália; Government Communications Security Bureau (GCSB) da Nova Zelândia)

obtiveram ‘comunicações internas’ do Brasil e da Colômbia); do programa BLACKPEARL, que interceptou conversas e *e-mails* da Petrobrás por meio de *crackear* sua rede virtual privada; de programas de escuta e interceptações de *e-mails* da presidenta Dilma Rousseff (o ex-presidente Luiz Inácio Lula da Silva teria irritado Washington ao convidar o então presidente do Irã, Mahmoud Ahmadinejad, para uma visita; quando Rousseff assumiu, mesmo distanciando de Teerã e recebendo Obama, a NSA interessou-se em adentrar o pensamento particular dela, espionando-a); e, por fim, por meio de obtenção de várias formas de acesso às embaixadas e consulados, especialmente em Washington, D.C e Nova York, sobretudo por via do programa SIGAD US-3136. O mapa a seguir (figura 3) mostra o volume titânico de dados coletados:

Figura 3 – Volume de dados rastreados pelo governo norte-americano



Fonte: Jornal *O Globo* (http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/)

No mapa, de cima para baixo, da esquerda para a direita, observa-se: BOUNDLESS INFORMANT / Visão geral (últimos 30 dias) /Total de DNI / Total de DNR / SIGADs (Designador de Atividade de Inteligência de Sinais) / Notações de caso / Sistemas de processamento / Cinco principais países (últimos 30 dias) / TOTAL / VISÃO DE PAÍSES / Estados Unidos (Greenwald, 2014).

Para Greenwald (2014), em última instância, além da manipulação diplomática e das vantagens econômicas, um sistema de espionagem onipresente permite aos EUA manter seu controle sobre o mundo, de modo que quando o país consegue saber tudo o que todos estão fazendo, dizendo, pensando e planejando – seus próprios cidadãos, populações estrangeiras, corporações internacionais, líderes de outros governos -, seu poder sobre eles é maximizado, o

que é duplamente verdadeiro quando o governo opera em níveis de sigilo cada vez mais altos, criando um espelho de apenas uma direção: o governo dos EUA vê tudo o que o resto do mundo faz, inclusive sua própria população, mas ninguém sabe de suas ações, dando lugar à mais perigosa de todas as condições humanas: o exercício de um poder ilimitado sem transparência nem prestação de contas.

Pelo exposto até aqui, é possível observar na linha do tempo da História, especialmente a partir da primeira revolução industrial, que a dinâmica das grandes potências, com destaque para a peculiaridade da formação dos EUA, insular e, consequentemente marcado pelo receio de invasões, esteve em constante interação, sendo ora causa, ora efeito de eventos históricos que modificariam ou redefiniriam sua política e/ou alterariam profundamente as técnicas e tecnologias relacionadas à segurança e à defesa. Para o caso que nos interessa, a espionagem, podemos observar que o desenvolvimento tecnológico, sobretudo nos períodos de guerra, acelerou mecanismos e formas de obtenção da informação de tal maneira que os estados econômica e militarmente mais avantajados, normalmente às custas dos periféricos, como mostra o contencioso da informática entre Brasil x EUA nos 1980, acabaram por dominar o setor e, no século XXI, como as revelações de Snowden puderam comprovar, vieram a usar a estrutura desigual de desenvolvimento acentuada pelas práticas neoliberais dos anos 1990, como mostram as privatizações das telecomunicações brasileiras nessa década, para, por meio da superioridade de suas empresas transnacionais e do controle de infraestrutura, monitorar e vigiar todos e tudo que pudesse vir a colocar em risco seu *status quo*.

É preciso observar, então, o que se esboça em termos de institucionalização e como o tema tem entrado no debate acadêmico, coisa que faremos a seguir.

3.2. INSTITUCIONALIZAÇÃO E DEBATE ACADÊMICO

Buzan (2012) nota que há quatro dimensões significativas na dinâmica dos debates acadêmicos para a evolução dos estudos de segurança e defesa: 1) os debates sobre epistemologia, metodologia e a escolha do enfoque da pesquisa que conduzem as Ciências Sociais; 2) a influência, nos estudos de defesa e segurança, do desenvolvimento de outras áreas acadêmicas; 3) a posição política e normativa dos estudiosos de segurança e defesa (a fronteira entre o acadêmico e o político, ou entre o estudioso e o conselheiro, seria sempre tênue e discutida; 4) a influência da ‘metavisão’ que os estudiosos mantêm sobre como uma área

deveria se desenvolver. Nesse sentido, para Buzan (2012) a institucionalização destaca mais ainda que os debates acadêmicos não devem se desdobrar em um vácuo econômico e estrutural, mas envolverem, além da alocação de recursos e da inserção de certo processo de reprodução, a dinâmica burocrática das organizações. Assim, a institucionalização é vista, para Buzan (2012), como sendo composta por quatro elementos que se entrelaçam: estruturas organizacionais (universidades, centros de pesquisa e *think-tanks*); financiamento (sem o apoio econômico, seria difícil vislumbrar como as organizações poderiam funcionar); disseminação do conhecimento (publicações); e redes de pesquisa (construídas por meio de associações profissionais, encontros durante conferências, intercâmbio de docentes e alunos através de programas de pesquisa, encaminhamentos de doutores graduados por professores antigos e pela comunicação diária de projetos de pesquisa).

Embora Buzan (2012) analise separadamente cada uma dessas forças motrizes, optamos em analisá-las em tópico único, já que a quantidade de debates e discussões acadêmicas tendo como temas os serviços de inteligência (e/ou a espionagem) no Brasil ainda não compõe um quadro claro de correntes ou propostas teóricas, observando-se, na verdade um grupo de pesquisadores na UFMG, um na UFRGS e outro na UFRJ. Também assim o fazemos diante da quase inexistência de institucionalização do tema no Brasil (faz-se aqui referência à carência de estruturas organizacionais, bem como de financiamento e redes de pesquisa envolvendo o tema, ou seja, especificamente para estudar serviços de inteligência ou espionagem), o que reflete a própria falta de consolidação dos serviços de inteligência brasileiros, obrigando-nos, neste tópico, a imaginar mais a influência e capacidade de atração que os impactos das denúncias de Snowden terão nos debates acadêmicos e na institucionalização, do que propriamente a discorrer sobre o que já existe.

Para Cepik (2001), o debate sobre o futuro das atividades de inteligência no Brasil arrasta-se fracamente desde a extinção do Serviço Nacional de Informações (SNI) em 1990; além disso, o duplo contexto de origem desse debate teria sido marcado pela transição para a democracia no plano nacional e pelas mudanças no ambiente de segurança internacional decorrentes do colapso da União Soviética e do fim da Guerra Fria, de modo que, depois de quase dez anos é que o impasse institucional teria sido resolvido com a criação da ABIN: em dezembro de 1999, o parlamento brasileiro aprovou a lei de criação da Agência Brasileira de Inteligência (ABIN) e do Sistema Brasileiro de Inteligência (SISBIN), sancionada em seguida pelo presidente da República. Mesmo assim, para Cepik (2001) pouca gente, no governo ou fora dele, manifestava (em 2001) uma formulação consistente sobre o que era, afinal, a atividade de inteligência tal como realmente praticada no Brasil e o que ela deveria ser no novo

contexto, na medida em que a institucionalização dos serviços de inteligência envolvia não apenas a obtenção de "estabilidade" organizacional, mas também um longo processo através do qual eles se tornariam (ou não) organizações "valiosas" para o público, o que implicaria um processo fortemente relacionado à transparência, ou seja, à capacidade do público ver e julgar por si mesmo os atos dos governantes na área de inteligência, de forma que mesmo que os serviços de inteligência contemporâneos viessem a tornar-se suficientemente ágeis para estabilizarem-se organizacionalmente no novo contexto internacional, sua eventual institucionalização dependeria ainda da difícil resolução do dilema da transparência.

Em relação às mudanças organizacionais mais importantes ocorridas depois da criação da ABIN, em 1999, e da queda das torres gêmeas, em 11 de setembro de 2001, Cepik (2005) destaca cinco transformações: a) subordinação da agência ao Gabinete de Segurança Institucional – GSI da Presidência da República; b) criação da Comissão Mista de Controle das Atividades de Inteligência – CCAI no Congresso; c) regulamentação da participação dos ministérios no âmbito do SISBIN; d) criação do Sistema de Inteligência de Defesa – SINDE; e) criação do Subsistema de Inteligência de Segurança Pública – SIPS.

Em 2008, a *Estratégia Nacional de Defesa* (END) tratou o ciberespaço[20] como um setor estratégico, ao lado dos setores espacial e nuclear (Brasil, 2008). Em agosto de 2010 o Comando do Exército Brasileiro iniciou a implementação do Centro de Defesa Cibernética do Exército (CD Ciber), com a missão de gerenciar e supervisionar o setor cibernético do Exército Brasileiro (Brasil, 2010a; 2010b).

Segundo Cepik et al. (2014), as portarias nº 666 e 667, de 2010, ambas do comandante do Exército, apenas puseram em funcionamento um "Núcleo de Defesa Cibernética no âmbito do Exército", submetido ao Departamento de Ciência e Tecnologia, já que a END, adotada pelo Brasil em 2008, atribuiu ao Exército o papel de integrar e coordenar as Forças Armadas do país no que diz respeito às atividades de defesa relativas ao setor cibernético. Por conta disso, segundo os autores (2014,) em 2011 e 2012, o Exército tomou medidas para aprofundar a institucionalização – inclusive pela via da adoção de um Decreto Presidencial – do Centro de Defesa Cibernética, previsto para funcionar plenamente em 2015; dessa forma, a segurança cibernética, no Brasil, entendida como uma atividade mais abrangente que a defesa, e mais

[20] Para Cepik et al. (2014) ciberespaço e Internet não são exatamente a mesma coisa: o primeiro precederia o desenvolvimento do segundo em décadas. Citando Kuehl, Cepik et al. (2014) assim definem o ciberespaço: um domínio operacional marcado pelo uso da eletroeletrônica e do espectro eletromagnético com a finalidade de criação, armazenamento, modificação e/ou troca de informações pelas redes interconectadas e interdependentes. Neste sentido, para eles (2014), as redes de telégrafo, radioamador, telefonia fixa e/ou móvel e televisão via satélite configuravam o ciberespaço muito antes do advento da Internet.

voltada para o estabelecimento de diretrizes e políticas de segurança a serem observadas na digitalização do Estado brasileiro, ficaria a cargo do Gabinete de Segurança Institucional da Presidência da República.

Após o caso Snowden em 2013, a avassaladora midiatização das revelações de espionagem acabou despertando o interesse pelos serviços de inteligência no Brasil. Este trabalho é em parte resultado deste interesse. A tendência que se vislumbra futuramente é a de aumento de pesquisas sobre o assunto, de maneira que a delação de Snowden acabará por se tornar em si mesmo um evento desencadeador de debates acadêmicos que, possivelmente, encaminharão para um maior grau de institucionalização da temática no Brasil. Alguns fatos ilustram essa tendência. Para Greenwald (2014), por exemplo, as revelações de Edward Snowden subverteram a perigosa dinâmica do exercício ilimitado de poder ao revelar a existência do sistema e seu modo de funcionamento. Pela primeira vez, pessoas do mundo inteiro puderam ter conhecimento da verdadeira extensão das capacidades de vigilância usadas contra elas.

A notícia provocou um debate mundial intenso e sustentado justamente porque essa vigilância representa uma grave ameaça à governança democrática. Ela também gerou propostas de reformas, uma discussão global sobre a importância da liberdade na internet e da privacidade na era eletrônica, além de uma conscientização sobre a pergunta vital: o que a vigilância sem limites significa para o indivíduo, em sua própria vida? Para Greenwald (2014), nos EUA, em termos práticos, isso pôde ser visto nos acontecimentos de uma única semana (em dezembro de 2013 – mais de seis meses após a primeira matéria do jornal The Guardian): a semana em questão começou com a drástica opinião emitida pelo juiz federal norte-americano Richard Leon de que a coleta de metadados pela NSA tinha probabilidades de ser considerada uma violação da Quarta Emenda constitucional dos EUA, e de que sua abrangência era "quase orwelliana"; e mais: o jurista, nomeado por Bush, observou de maneira pertinente que "o governo não citava nenhum caso em que a análise da coleta em massa de dados pela NSA tenha de fato impedido uma ação terrorista iminente"; apenas dois dias depois, uma comissão consultiva criada pelo presidente Obama quando o escândalo da NSA veio a público emitiu um relatório de 308 páginas sobre a questão; esse relatório também rejeitava de forma decisiva as alegações da agência quanto à importância vital de sua espionagem: "Nosso documento sugere que as informações somadas às investigações sobre o terrorismo pelo uso da seção 215 (da Lei Patriota) a respeito de metadados de telefonia não foi essencial para impedir atentados", afirmou a comissão, confirmando que em nenhum caso o desfecho teria sido diferente "sem o programa de coleta de metadados de telefonia da seção 215".

Enquanto isso, fora dos EUA, as repercussões também foram impactantes: a Assembleia Geral da ONU de 2013 votou por unanimidade a favor de uma resolução – apresentada por Alemanha e Brasil – segundo a qual a privacidade na internet seria um direito humano fundamental, aprovação considerada por um especialista como "um recado contundente aos EUA de que estava na hora de reverter o curso e pôr fim à vigilância generalizada da NSA". Coincidentemente, para Greenwald (2014), o Brasil anunciou que não escolheria a Boeing, empresa baseada nos EUA, para um aguardado contrato de compra de jatos de caça no valor de 4,5 bilhões de dólares, mas sim a companhia sueca Saab; para Greenwald (2014), a indignação brasileira com a espionagem de seus líderes, empresas e cidadãos conduzida pela NSA foi claramente um fator-chave nessa decisão surpreendente[21]: "O problema da NSA estragou tudo para os americanos", teria dito à Reuters uma fonte do governo brasileiro. No discurso inflamado na ONU, em setembro de 2013, a presidenta Dilma Rousseff disse que a "rede mundial de espionagem eletrônica" dos EUA estava agora exposta e causava repulsa em todo o mundo, pois a "intromissão" desta rede não era apenas uma afronta às relações entre Estados amigos, como também uma flagrante violação do direito internacional, desconsiderando o conceito de que a NSA estivesse de alguma forma lutando contra o terrorismo: "O Brasil sabe como se proteger" disse.

Para Harding (2014), não foi surpresa a presidenta Dilma Rousseff reagir negativamente à espionagem da NSA, vendo-a como uma violação escandalosa à soberania do Brasil: a Casa Branca reagiu a suas reclamações com respostas genéricas, nos mesmos moldes das fornecidas a alemães e franceses e, em setembro de 2013, Rousseff anunciou que estava cancelando sua visita oficial a Washington, que deveria ocorrer em 23 de outubro de 2013, a despeito da tentativa de Obama de demovê-la da ideia (na falta de "tempo para uma investigação oportuna [...] não há condições para que essa viagem seja feita", declarou o governo brasileiro).

Harding (2014) acredita que no início de 2014 teria ficado claro que o impacto das revelações de Snowden era muito maior do que aquele causado pelo WikiLeaks. A publicação, pelo WikiLeaks, no final de 2010, dos telegramas secretos de diplomatas norte-americanos por todo o mundo claramente teria tido, para Harding (2014) consequências: meia dúzia de embaixadores foram forçados a abrir mão de seus postos; comunicados vazados serviram para

---

[21] Apesar do argumento de Greenwald (2014), para Lucas Kerr de Oliveita et al. (Isape Blog) a escolha do Gripen NG sueco foi baseada estritamente em autonomia tecnológica (aeronave mais favorável às necessidades brasileiras) e estratégica (o grande trunfo do Gripen estaria na disposição da Suécia em transferir tecnologias sensíveis e desenvolvê-las conjuntamente com o Brasil). (***Gripen NG: a decisão pela autonomia tecnológica e estratégica, 27.12.2013 - https://isape.wordpress.com/2013/12/27/gripen-ng-a-decisao-pela-autonomia-tecnologica-e-estrategica/***)

alimentar a Primavera Árabe, cristalizando o ressentimento popular contra regimes na Tunísia, na Líbia e no Egito; além disso, nem todas as consequências haviam sido negativas: paradoxalmente, houvera melhora na reputação do serviço estrangeiro dos EUA; diplomatas norte-americanos, de modo geral, saíram na história como inteligentes, íntegros e trabalhadores; alguns tinham verdadeiro talento literário.

Com os arquivos Snowden, entretanto, os efeitos foram mais profundos, segundo Harding (2014): era como se o mundo estivesse se reordenando de forma lenta e nem sempre coerente – digerindo a ideia de que os EUA estavam espionando não apenas líderes estrangeiros, mas populações civis inteiras; a questão, tanto para os aliados europeus quanto para poderes autoritários rivais, era: como reagir? A NSA parecia enxergar aliados próximos dos EUA, com quem valores e história eram compartilhados, como se não estivessem de forma alguma do mesmo lado. Pelo contrário, eram, nas palavras de Harding (2014), 'aminimigos', cujas reações obedeceram a várias tendências:

a) Angela Merkel fez um apelo por uma regulação na espionagem entre os parceiros, pois, nos estágios iniciais do caso Snowden, a NSA tentou remediar a situação, mas Merkel e François Hollande diziam querer que um novo acordo transatlântico de não espionagem fosse negociado até o final de 2013, sendo que o Reino Unido e outros países da União Europeia estariam livres para se inscrever nesse novo código de conduta, que regularia o comportamento dos serviços de segurança e inteligência;
b) o presidente da Indonésia ficou furioso com o comportamento nada amistoso de sua vizinha Austrália e rebaixou as relações diplomáticas com Canberra e cessou a cooperação em questões como o contrabando de pessoas e a tentativa de imigração por embarcações ilegais;
c) o tema dominou uma cúpula da União Europeia em Bruxelas, com Merkel comentando que a questão em jogo não era o seu celular, mas o que ele representava – "os telefonemas de milhões de cidadãos europeus"; os políticos alemães pediram a suspensão das negociações de um acordo comercial com os EUA até que a Casa Branca desse uma resposta satisfatória; houve solicitações para que fossem tomados depoimentos testemunhais de Snowden em Moscou e para que lhe fosse concedido asilo (algo que Merkel já havia recusado);
d) David Cameron viu-se alvo de críticas veladas, recusando-se a informar se o GCHQ estivera envolvido em escutas de alto-escalão, ou se tinha tido acesso ao material interceptado do celular de Merkel;
e) parlamentares europeus votaram novas e duras regras para a privacidade de dados, com o objetivo de impedir que dados recolhidos na União Europeia por empresas como Google, Yahoo ou Microsoft acabassem nos servidores da NSA: a proposta, uma contraofensiva

explícita ao PRISM, visava restringir o compartilhamento de informações da União Europeia com países de fora do bloco, propondo também que cidadãos europeus tivessem o direito de apagar seus registros digitais da internet, bem como grandes multas para as empresas que quebrassem essas regras;

f) a nova palavra de ordem era "cibersoberania": o objetivo comum entre os aliados descontentes dos EUA era tornar mais difícil para a NSA ter aceso a seus dados nacionais (para Harding (2014), a países autoritários como a Rússia, isso representava um bônus, já que um maior controle estatal sobre a internet tornava mais fácil espionar seus próprios cidadãos e abafar a dissidência);

g) a reação mais veemente, para Harding (2014), veio do Brasil: em outubro, a presidenta Dilma Rousseff anunciou planos para a construção de um novo cabo submarino ligando a América do Sul à Europa, excluindo, em tese, os EUA da triangulação das comunicações, tornando mais difícil para a NSA obter informação brasileira; a presidenta também ponderou sobre uma legislação que forçaria o Google e outros gigantes da tecnologia dos EUA a armazenar dados de usuários brasileiros em servidores locais; ao mesmo tempo, milhares de servidores federais foram obrigados a adotar uma forma de *e-mail* altamente criptografada;

h) as divulgações de Snowden pareciam ter disparado o que o CEO (diretor) do Google, Eric Schimidt, apelidou de 'balcanização' da internet, já que o que era para ser uma ferramenta universal estava sob ameaça de se tornar algo fragmentado e 'específico para cada país';

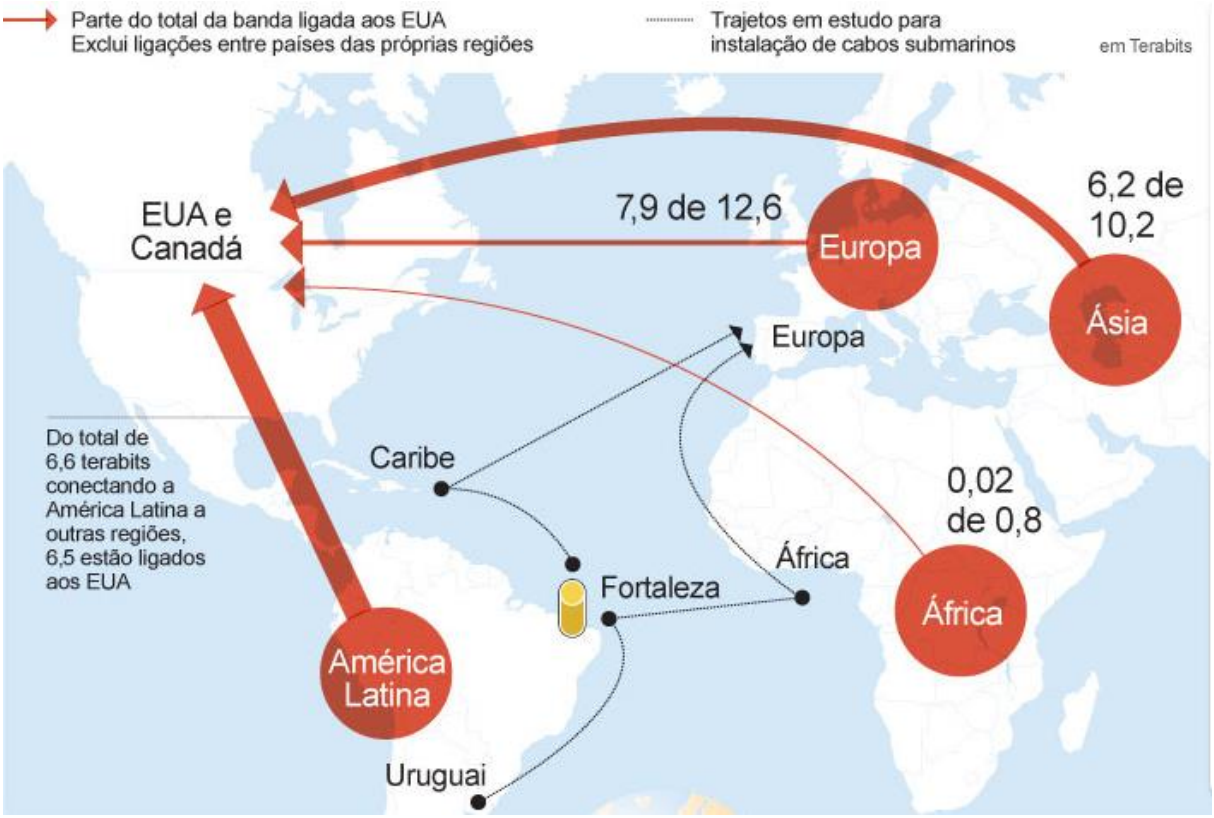
i) na Alemanha, a estatal Deutsche Telekom desenterrava planos para uma nova rede nacional de internet, com o slogan 'e-mail made in Germany', sugerindo a seus consumidores que o *e-mail* desenvolvido por eles seria tão confiável quanto os eletrodomésticos feitos na Alemanha e dando a entender que os *e-mails* entre usuários alemães não precisariam passar por servidores nos EUA, uma vez que o tráfego, em sua maior parcela, seria mantido dentro da área de Schengen da União Europeia (que convenientemente exclui a Grã-Bretanha), com a aspiração de manter-se a salvo dos espiões anglófonos intrometidos;

j) a consequência mais inesperada do caso Snowden talvez tenha sido, para Harding (2014), o retorno da máquina de escrever, especialmente na Índia e na Rússia, obrigando aqueles que se preocupavam com a privacidade a retornarem à era pré-internet.

A despeito das ações mais ou menos retóricas e/ou mais ou menos pragmáticas, o fato é que o volume de informações acessadas pelos EUA foi o que fez a diferença para casos de delações anteriores, inserindo a prática da espionagem em patamares dificilmente analisados fora de escala. Se a economia de escala é aquela que organiza o processo produtivo de maneira que se alcance a máxima utilização dos fatores produtivos envolvidos, pode-se dizer que o caso

Snowden revelou uma “espionagem de escala”, ou seja, aquela que mobiliza todo o processo de inteligência de modo a alcançar a máxima utilização da tecnología disponível. O mapa a seguir (figura 4) mostra o volume de rastreamento do governo norte-americano, por região:

Figura 4 – Conexão com os EUA por região



Fonte: Jornal *O Globo* (http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/)

Observa-se que, embora tenha diminuído sua influência sobre a região, os EUA ainda são o destino por que passam 86% das conexões de internet da América Latina.

A repercussão do caso Snowden, no Brasil, contribuiu para a aprovação do Marco Civil da Internet (oficialmente chamado de Lei nº 12.965, de 23 de abril de 2014), que regula o uso da Internet nacionalmente, por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado. Efeito direto da influência da espionagem de 2013 é o capítulo III (da provisão de conexão e de aplicações de internet), seções I (da neutralidade de rede), II (da proteção aos registros, aos dados pessoais e às comunicações privadas), III (da responsabilidade por danos decorrentes de conteúdo gerado por terceiros) e IV (da requisição judicial de registros), em que se centra especialmente no respeito ao sigilo das comunicações, na privacidade e inviolabilidade dos

dados, não só exigindo esclarecimentos expressos, mas também detalhes sobre coleta, uso, armazenamento e tratamento de dados pessoais.

A interconexão entre a política das grandes potências, os eventos, a tecnologia, os debates acadêmicos e a institucionalização de uma temática na área de segurança e defesa é visível quando observamos o processo por meio do qual vem se dando a securitização[22] do espaço virtual: marcados pelo estreito vínculo entre o Estado e as grandes corporações, os EUA industrializaram-se rapidamente, hospedando grande parte da Segunda Revolução Industrial e sendo os precursores, junto com o Japão, a quem ofereceu assistência após a Segunda Guerra Mundial, da Terceira Revolução Industrial (ou Tecnológica), o que lhes deu praticamente o monopólio do suporte físico da Sociedade em Rede, consolidada com a participação vitoriosa na Primeira Guerra Mundial, com a saída da Segunda Guerra Mundial como superpotência e com a hegemonia após o Fim da Guerra Fria; tais eventos incrementaram a estrutura tecnológica norte-americana, retroalimentada, de um lado, pelas guerras que exigiam constante desenvolvimento de novas tecnologias (depois adotadas fora do contexto militar, como a internet), e, de outro, pelos *think tanks*, universidades, organizações, empresas, redes de pesquisadores e vultuosos financiamentos para investigações mais sobre Estudos Estratégicos e menos, mas também, sobre a Estudos da Paz, garantindo a institucionalização do tema em solo estadunidense - origem de grande parte das primeiras teorias de relações internacionais - simultaneamente a uma incomparável consolidação como maior potência militar, econômica e cibernética, neste último caso especialmente por hospedar a maior parte dos pontos de redistribuição dos sinais de internet por meio de cabos submarinos (no caso brasileiro[23], atualmente, há cinco cabos submarinos ligando o Brasil ao exterior, sendo que quatro deles vão para os EUA e apenas um para a Europa).

A história brasileira, com suas especificidades, e associada a uma posição desigual do Brasil em um sistema econômico marcado pela exploração das periferias pelos grandes centros, mostra que os avanços (a partir dos anos 2000), recuos (durante a ditadura militar) ou estagnação (entre a redemocratização e os anos 2000) na constituição de serviços de inteligência livres de influências externas estiveram quase sempre atrelados (positiva ou negativamente) às

---

22 A securitização e os critérios para securitização, segundo o grupo de Copenhague, são práticas intersubjetivas, por meio das quais um agente securitizador procura estabelecer socialmente a existência de uma ameaça à sobrevivência de uma unidade (BUZAN et al., 1998).

23 A Telebrás aprovou em 15.01.2014 a criação de uma empresa com capital misto em parceria com a espanhola IslaLink para construir e operar um novo cabo submarino de fibra óptica dedicado a transmitir dados de internet entre o Brasil e a Europa. O investimento foi de US$ 185 milhões (R$ 435 milhões) e a estrutura deverá ficar pronta em 2016, sem passar pelos EUA (publicado em Olhar Digital - em 16/01/2014 às 11h30, endereço eletrônico: http://olhardigital.uol.com.br).

políticas dos EUA para o continente, o que dificultou a geração precoce tanto de teorias próprias de relações internacionais, como de debates acadêmicos e de institucionalização sobre os serviços de inteligência de modo geral e a espionagem de forma particular.

A divisão de recursos tanto na área de inteligência quanto na área dos estudos de inteligência reflete em parte, como concluiu Cepik (2005), uma outra decisão altamente problemática, a de priorizar quase que exclusivamente os problemas de segurança domésticos ou internos, em detrimento da coleta e análise de inteligência sobre segurança internacional. A espionagem norte-americana revelada por Snowden ilustra a consequência dessa escolha brasileira, expondo as fragilidades das ações de contra-inteligência da Abin, ou seja, a incapacidade de ter previsto os aberrantes atos de monitoramentos da NSA, disseminando entre os brasileiros – Estado e sociedade – a sensação de não deter a soberania sobre o próprio território. A soberania nacional, a seguir, é justamente o último item desta pesquisa.

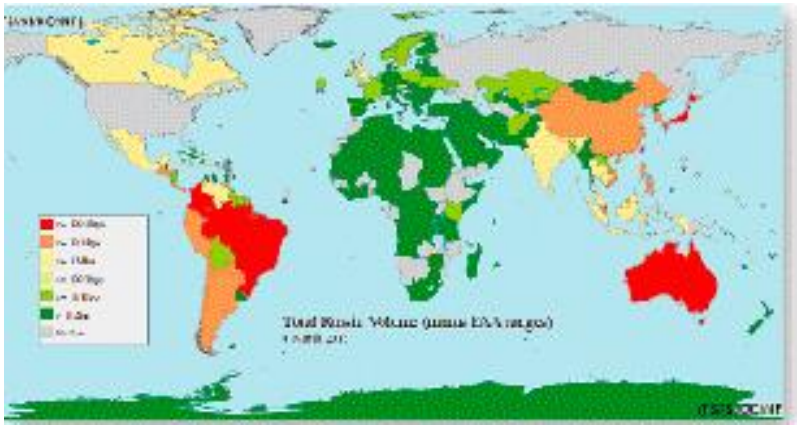
3.3. SOBERANIA

Como demonstrado ao longo deste trabalho, especialmente no item 1, os serviços secretos sempre existiram e é ilusão pensar que a extrapolação de suas atividades de obtenção de dados legais e a consequente prática de espionagem cessarão. Assim sendo, como defende Cepik (2001) caberia a cada país desenvolver meios mais eficientes para se defender da espionagem externa, já que a inteligência é uma das atividades fundamentais de qualquer Estado e tem reflexos diretos sobre o bem-estar de todos os cidadãos, sendo a partir de dados de inteligência que o Estado planeja e executa políticas públicas de defesa nacional, segurança pública e relações exteriores. A delação de Snowden além de revelar os interesses ocultos dos EUA no cenário internacional também expôs a fragilidade dos países espionados no que tange a não perceber detalhadamente como seus dados sensíveis vinham sendo, desde um tempo considerável, monitorados e avaliados, o que gerou muita celeuma em torno do tema. No Brasil, as respostas às vigilâncias foram inflamadas e houve acusações de que os EUA teriam violado a soberania nacional.

Isso ocorreu especialmente depois de 6 de julho de 2013, quando o jornal brasileiro O Globo publicou reportagem que apontava que milhões de chamadas telefônicas e *e-mails* de brasileiros e estrangeiros no Brasil tinham sido monitorados pelo programa de vigilância norte-americano. Os mapas a seguir (figuras 5, 6 e 7) demonstram que o Brasil constituía um alvo

importante para os EUA. Os mapas ilustram a quantidade de mensagens e telefonemas trocados por vários países do mundo com Rússia, Paquistão e Irã, compilados pelo programa Fairview, aparentemente nos dias 4 e 5 de março de 2013. Os países em vermelho, laranja e amarelo tiveram o maior número de mensagens rastreadas. Em todos os mapas, o Brasil se destaca entre os países da América Latina:

Figura 5 – Rastreamento de mensagens trocadas com Rússia

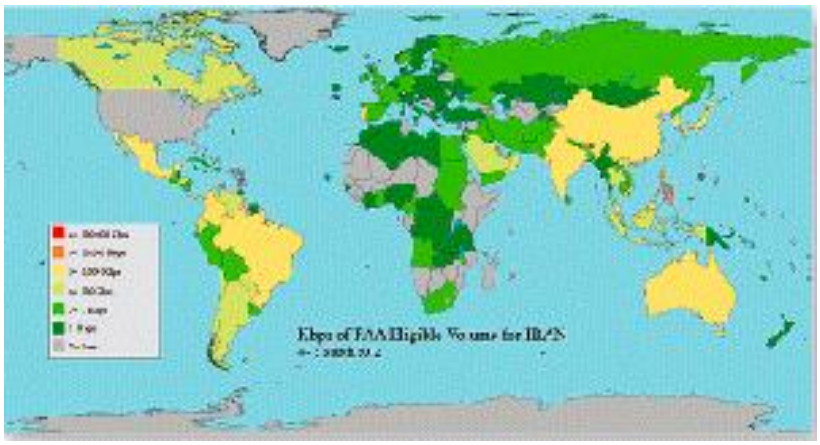


Fonte: Jornal *O Globo* (http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/)

Figura 6 – Rastreamento de mensagens trocadas com Paquistão

Fonte: Jornal *O Globo* (http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/)

Figura 7 – Rastreamento de mensagens trocadas com Irã



Fonte: Jornal *O Globo* (http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/)

A indignação aumentou na medida em que os documentos apontaram também que uma estação de espionagem da NSA funcionou em Brasília pelo menos até 2002 e que a embaixada do Brasil em Washington, além da representação na ONU, em Nova York, também poderiam ter sido monitoradas. Pelas matérias jornalísticas, soube-se também que outros países da América Latina tinham igualmente sido monitorados (situações similares teriam ocorrido no México, Venezuela, Argentina, Colômbia e Equador). Os alvos da vigilância, como a Petrobrás e o Ministério de Minas e Energia, sugeriam que o interesse dos EUA não se circunscrevia apenas a assunto militares, mas também em relação ao petróleo e à produção de energia. Em 7 de julho de 2013, o então ministro das Relações Exteriores, Antônio Patriota, disse que o governo solicitaria esclarecimentos aos EUA e ao embaixador americano no Brasil. Algumas das possíveis respostas brasileiras, como a suposta influência na compra de aviões da empresa sueca Saab e o adiamento de viagem da presidenta Dilma Rousseff aos EUA, foram já abordadas no item anterior, com o intuito de ilustrar as várias dimensões que o tema abrangeu, incluindo uma maior disseminação da temática na comunidade acadêmica e instituições diversas. Neste tópico examina-se um pouco mais detidamente em que grau a espionagem estadunidense de fato poderia ter violado a soberania brasileira, já que o artigo primeiro da Constituição registra que a República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como primeiro fundamento a soberania.

Em uma perspectiva histórica, a teoria da soberania manifestou quatro grandes papéis:1) durante o Feudalismo, quando correspondia à dominação do senhor sobre seu feudo; 2) no Absolutismo, quando justificava o poder absoluto do rei, servindo como seu instrumento (Jean Bodin (1530-1596) defendeu que a soberania refere-se à entidade que não conhece superior na

ordem externa nem igual na ordem interna); 3) no Iluminismo, quando o poder monárquico foi contestado; e 4) após o século XVIII, quando a centralidade do rei seria substituída pela do direito do povo (Jean-Jacques Rousseau transfere o conceito de soberania da pessoa do governante para todo o povo, entendido como corpo político ou sociedade de cidadãos, sendo a soberania inalienável e indivisível e devendo ser exercida pela vontade geral, denominada por soberania popular). Foi, portanto, a partir do Estado Moderno, com o esplendor da Revolução Francesa, que o conceito de soberania começou a ser concebido e, pouco a pouco, em uma evolução histórica, foi lapidado, chegando tal qual se vislumbra hoje.

A partir do século XIX é elaborado um conceito jurídico de soberania, segundo o qual a soberania não pertenceria a nenhuma autoridade particular, mas ao Estado enquanto pessoa jurídica. E é a noção jurídica de soberania, atualmente, que orienta as relações entre Estados e enfatiza a necessidade de legitimação do poder político pela lei. Entretanto, a soberania tem uma significação bastante complexa e não deveria ser definida exclusivamente através de uma concepção jurídica nem por uma concepção unicamente social, sendo um problema sócio-jurídico-político. Para Reale (2000):

> "Soberania é tanto a força ou o sistema de forças que decide do destino dos povos, que dá nascimento ao Estado Moderno e preside ao seu desenvolvimento, quanto a expressão jurídica dessa força no Estado constituído segundo os imperativos étnicos, econômicos, religiosos etc., da comunidade nacional, mas não é nenhum desses elementos separadamente: a soberania é sempre sócio-jurídico-política, ou não é soberania. É esta necessidade de considerar concomitantemente os elementos da soberania que nos permite distingui-la como uma forma de poder peculiar do Estado Moderno". (REALE, 2000, p.139).

A partir desta concepção, por meio da qual se pode relacionar soberania com autonomia, a intervenção clandestina de um Estado em outro pode constituir grave fator de desestabilização e violação desta autonomia, vez que, no caso de espionagem, por exemplo, informações fundamentais obtidas secretamente poderiam ser utilizadas estrategicamente pelo Estado invasor, rebaixando consideravelmente o poder de ação (e mesmo reação) do Estado invadido. Nesse sentido, a autonomia do Estado invadido para organizar-se e gerir-se com o objetivo do bem comum estaria, assim, seriamente comprometida num cenário em que o Estado-espião venha a ser a maior potência do globo. Dessa forma, a ideia de uma sociedade organizada, constituída por um Estado independente é reflexo da soberania e da capacidade de auto determinar-se, que ficariam seriamente prejudicados com a prática abusiva da espionagem.

Tirante essa perspectiva, a informação na Sociedade em Rede equivale a um recurso de poder, podendo ser comparado às riquezas naturais de um país. Se um Estado, por exemplo,

decide interferir no sistema informatizado de eletricidade de várias capitais e cidades de outro Estado, poderá provocar um apagão generalizado, causando inúmeros prejuízos. A confirmação de que isso é possível pode ser vista na operação Stuxnet, em 2009, quando EUA e Israel quase causaram um acidente comparável a Chernobil, ao tentar atingir o sistema operacional desenvolvido pela empresa Siemens para controlar as centrífugas de enriquecimento de urânio iranianas. O Stuxnet é um *worm*[24] de computador e foi descoberto em junho de 2010 pela empresa bielorrussa desenvolvedora de um antivírus (VirusBlokAda). Foi o primeiro *worm* descoberto que espionava e reprogramava sistemas industriais. Foi especificamente escrito para atacar um sistema de controle industrial utilizado para controlar e monitorar processos industriais, sendo capaz de reprogramar controladores lógicos programáveis e esconder as mudanças, além de poder aparecer camuflado em mais de 100 mil computadores.

Greenwald (2014) registra que, embora a coleta *upstream* (a partir de cabos de fibra ótica) e a coleta direta nos servidores das empresas de internet (programa PRISM) tenham fornecido a maioria dos registros obtidos pela NSA, a agência realiza também o que chama de Exploração de Rede Computacional (CNE), inserindo *malwares* em computadores específicos para vigiar seus usuários, de modo que quando consegue inseri-los, a NSA torna-se, no jargão da agência, 'dona' do computador, passando a ver cada tecla digitada a cada tela visualizada; A divisão responsável por esse tipo de manobra, Operações de Acesso Customizado (TAO), é, segundo Greenwald (2014), na realidade, a unidade de *hacking* interna da agência. Com base nos documentos de Snowden, o jornal New York Times noticiou que a NSA implantou malwares "em quase 100.000 computadores espalhados pelo mundo" (Greenwald, 2014).

Agrava mais ainda o quadro o domínio que os EUA detêm sobre os servidores de gestão de cibersegurança. Para Pires (2012), o atual modelo unilateral de governança da Internet, constituído desde 1998, pelo Departamento de Comércio dos Estados Unidos, pela ICANN (Corporação da Internet para Atribuição de Nomes e Números - *The Internet Corporation for Assigned Names and Numbers*, em Inglês) e pela VeriSign (uma empresa que atua na área de segurança de redes, internet e telecomunicações), foi o resultado de uma política de dominação voltada para consolidar uma nova forma de imperialismo digital, compelido pela mundialização

[24] Um *worm* (termo da língua inglesa que significa, literalmente, "verme") é um programa autorreplicante, semelhante a um vírus. Enquanto um vírus infecta um programa e necessita deste programa hospedeiro para se propagar, o *worm* é um programa completo e não precisa de outro para se propagar. Um *worm* pode ser projetado para tomar ações maliciosas após infestar um sistema. Além de se autorreplicar, pode deletar arquivos em um sistema ou enviar documentos por *e-mail*.

e o crescimento comercial da internet. Pires (2012) acredita que o desenvolvimento dessa política de imperialismo digital, a partir do controle dos servidores da zona raiz da Internet pela tríade: Departamento de Comércio, ICANN e VeriSign, fez emergir uma nova forma de dominação jurídica, econômica, tecnológica e cultural. Neste sentido a ICANN através da IANA (*The Internet Assigned Numbers Authority*), continua controlando a concessão de Registros Regionais da Internet (*Regional Internet Registry - RIR*). A figura 8 localiza os treze principais servidores da zona raiz da internet:

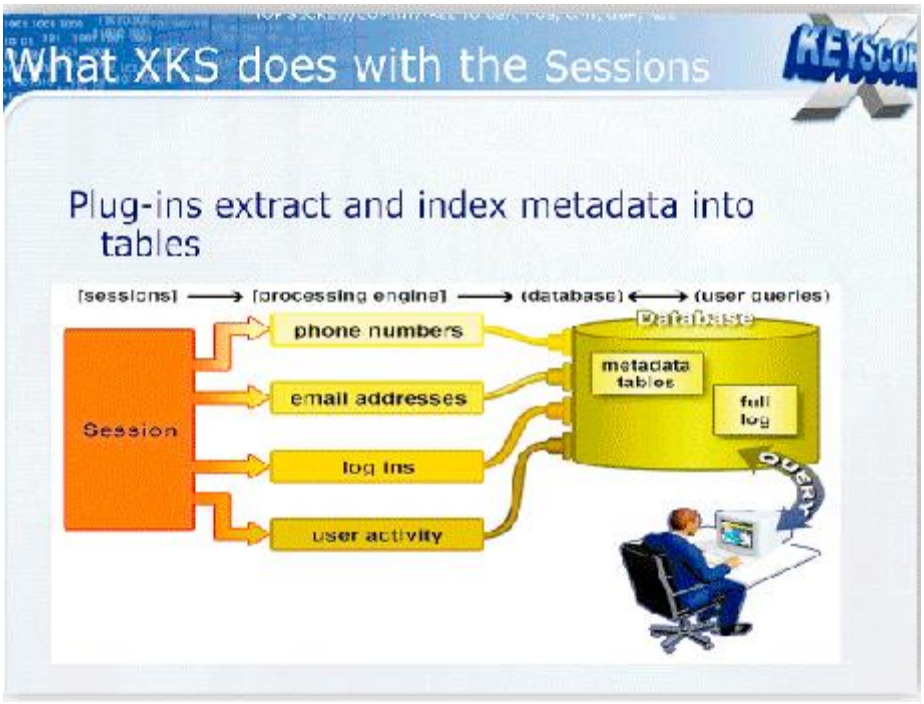
Figura 8. Localização Geográfica dos treze principais Servidores da Zona Raiz da Internet.

Elaboração: PIRES, Hindenburgo Francisco (2012).

Pires (2012) explica que os treze servidores da zona raiz são identificados pelas letras do alfabeto de A a M. Dos treze servidores da zona raiz dez, estão localizados fisicamente nos Estados Unidos (A, B, C, D, E, F, G, H, J, L); destes, 6 operam dentro do ciberespaço estadunidense (A, B, D, E, G, H), voltados para garantir a gestão do sistema de cibersegurança, os quatro outros são servidores anfitriões (C, F, J, L) que operam com sistema de endereçamento descentralizado *Anycast*, viabilizando o acesso a um aglomerado de servidores comerciais secundários replicantes distribuídos por vários países, fisicamente instalados fora da região de influência dos servidores da zona raiz da Internet nos EUA. Os três servidores restantes da zona raiz que operam fora do território dos EUA (I, K, M), localizados respectivamente na Holanda, na Suécia e no Japão, são servidores anfitriões que operam com sistema de endereçamento descentralizado (*anycast*) e também permitem o acesso de centenas de servidores secundários replicantes de outras regiões.

Como se observa, os governos têm serviços de inteligência, cuja extrapolação das funções geram a espionagem, porque esperam maximizar poder através do desenvolvimento de capacidades de inteligência. No caso Brasil x EUA em 2013, entretanto, essa maximização, sob vários aspectos, pode ser questionada e se constituir em violação da soberania nacional. Em uma sequência de reproduções de *Power Point* vazadas por Snowden, duas imagens chamam a atenção. Na primeira (figura 9), vê-se como funciona o sistema de espionagem com grampos em linhas telefônicas, *e-mails* e outros dados, que são mandados à sede, em Utah:

Figura 9 – Funcionamento do programa X-KEYSCORE

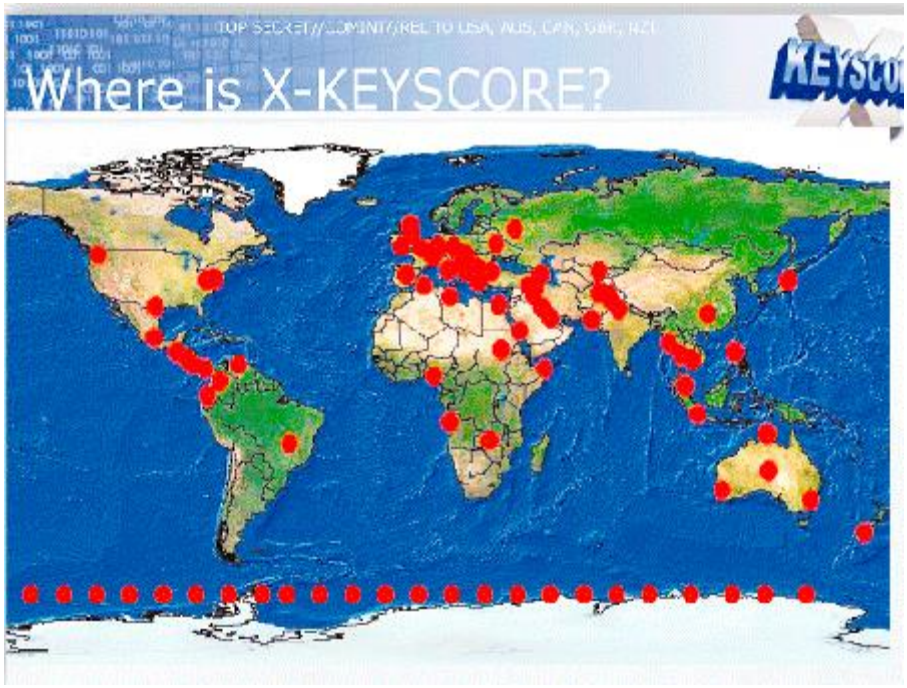


Fonte: Jornal *O Globo* (http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/)

De cima para baixo, da esquerda para a direita observa-se: "O que o XKS faz com as sessões / Extração de plug-ins e indexação de metadados em tabelas (sessões) / (mecanismo de processamento) / (base de dados) / (solicitações de usuários) / Sessão / números de telefone / endereços de e-mail / logins / atividade do usuário / Base de dados / tabelas de metadados / log completo / solicitação" (Greenwald, 2014).

Na segunda (figura 10), percebe-se que no mapa de 2008 o Brasil está dentre os países bisbilhotados pelo programa X-KEYSCORE, que detecta a presença de estrangeiros através da língua usada em e-mails e telefonemas:

Figura 10 – Mapa de rastreamento do programa X- KEYSCORE



Fonte: Jornal *O Globo* (http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/)

Lê-se, "Onde está o X-KEYSCORE?" (tradução livre).

Greenwald (2014) explica que o principal programa usado pela NSA para coletar, classificar e pesquisar informações, que começou a ser usado em 2007, é o K-KEYSCORE, que permitiu um salto radical no escopo dos poderes de vigilância da agência, fazendo-a qualificá-lo de sistema 'de maior alcance' para a coleta de dados eletrônicos. Segundo Greenwald (2014), um documento preparado para o treinamento de analistas alega que o programa capa 'praticamente tudo o que um usuário típico faz na internet', incluindo texto contido em e-mails e atividades, buscas no Google e o nome dos sites visitados. Centrar-nos-emos especialmente nas interceptações telefônicas e de *e-mails*.

Primeiramente, sob o aspecto da Declaração Universal dos Direitos Humanos, de 1948, os EUA teriam violado os artigos 12 e 19:

> "Art. 12: Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.
>
> Art. 19: Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão. "

Sob o aspecto da Declaração Americana dos Direitos e Deveres do Homem, também de 1948, teria havido a violação dos artigos 5º, 9º e 10º (Resolução XXX, Ata Final, aprovada na IX Conferência Internacional Americana, em Bogotá, em abril de 1948):

> "Artigo 5º: Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar.
>
> Artigo 9º: Toda pessoa tem direito à inviolabilidade do seu domicílio.
>
> Artigo 10º: Toda pessoa tem direito à inviolabilidade e circulação da sua correspondência."

Chama a atenção o fato de que na Nona Conferência Internacional Americana, que se reuniu em Bogotá (Colômbia), em 1948, vinte e um Estados (incluindo EUA e Brasil, evidentemente) adotaram a Carta da Organização dos Estados Americanos, o Tratado Americano sobre Soluções Pacíficas ("Pacto de Bogotá") e a Declaração Americana dos Direitos e Deveres do Homem. Na mesma conferência foi adotado o Acordo Econômico de Bogotá, que buscava promover a cooperação econômica entre os Estados americanos, contudo, curiosamente este nunca entrou em vigor.

Sob o aspecto da legislação brasileira, a Constituição brasileira considera crime realizar interceptação de comunicações telefônicas, de informática ou telemática sem autorização judicial, prevendo a inviolabilidade das comunicações telefônicas, salvo nos casos de investigação de crimes e devidamente autorizada por juiz. A norma é regulamentada pela lei 9296/96. A partir do advento dessa lei, tornou-se possível a interceptação telefônica quando houver indícios de participação em crime punido com pena de reclusão e não houver outro meio de prova para se chegar a autoria e materialidade da infração. A ABIN, por exemplo, fora desses casos, não pode solicitar ou executar interceptação telefônica (de dados ou metadados). Nesse sentido, os EUA teriam violado os artigos primeiro e segundo da lei brasileira:

> "Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
>
> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.
>
> Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
>
> I - não houver indícios razoáveis da autoria ou participação em infração penal;
>
> II - a prova puder ser feita por outros meios disponíveis;
>
> III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.
>
> Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e

> qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada."

O problema que se coloca é: mesmo tipificado o ato, como aplicar a lei se o acusado que efetuou a ação pertence a outro Estado ou é o próprio Estado, nesse caso o mais poderoso do sistema? Foge ao escopo desse trabalho responder a essa questão, pois claramente a 'punição' da violação da soberania brasileira pelos EUA dificilmente se efetivaria. Quando Milton Santos investigou a Geografia das Redes, concluiu que as redes inscritas no território, ao mundializarem-se, apresentavam características topológicas que favoreciam a extrapolação dos seus limites físicos. Este processo traria implicações que afetaria o espaço soberano das fronteiras, tendo em vista que as redes eram "os mais eficazes transmissores do processo de globalização a que assistimos" (Santos, 2008). O que se observou no caso da espionagem envolvendo o Brasil e os EUA foi essa nítida contradição entre dois Estados soberanos diluídos na geografia das redes: legislações de ambos os lados foram violadas, um ao espionar, violando sua própria legislação, e outro ao ser espionado, tendo seu corpo jurídico ignorado pelo Estado espião. De qualquer maneira, entretanto, nem a punição da violação nem a solução para o dilema esboçam estar no recrudescimento de nacionalismos e, consequentemente, das soberanias, pelo contrário, sugerem um questionamento delas.

Dessa forma, o vazamento de informações sobre as operações de interceptação e vigilância dos Estados Unidos contra diversos países e regiões, incluindo o Brasil, deve demonstrar que o desenvolvimento tecnológico na era digital cria novos desafios, riscos e oportunidades para os países. E, se na guerra e na paz, as atividades de inteligência dos Estados seguirão existindo no século 21, então, como sugere Cepik (2001), o Brasil deve conceber as atividades de inteligência como uma função de seus recursos e de suas necessidade, de modo que abstraia a antiga visão de inteligência concebida pelo Sistema Nacional de Informações [de ter obsessiva preocupação com inimigos internos] e, entre as várias missões que os órgãos de inteligência podem receber em diferentes contextos, apoie o planejamento de capacidades defensivas e o desenvolvimento e/ou aquisição de sistemas de armas, de acordo com o monitoramento das sucessivas inovações e dinâmicas tecnológicas dos adversários. Também se espera, conforme aconselha Cepik (2001), que a inteligência seja capaz de subsidiar o planejamento militar e a elaboração de planos de guerra, bem como de apoiar as operações militares de combate e outras (operações de paz, assistência, missões técnicas etc.), além de alertar os responsáveis civis e militares contra ataques-surpresa (do tipo o revelado por Snowden), surpresas diplomáticas e graves crises políticas internas que podem nunca ocorrer, mas para as quais os governantes devem preferir 'assegurar-se' em vez de arriscar, e, por fim,

compreender que atos de sabotagem, ataques cibernéticos e operações de guerra eletrônica são atos de guerra, uma alternativa de alto custo para qualquer Estado.

Nessa lógica, afora a otimização dos serviços de inteligência brasileiros, que devem estar preparados para enfrentar atos de espionagem, cremos que o contexto internacional atual (em parte descrito ao longo do trabalho), indiciam que as ações isoladas de segurança ou contra-inteligência por parte de um país, especialmente de um em desenvolvimento, pouco tendem a ter efeitos reais sobre o complexo, integrado e abrangente sistema de monitoramento estadunidense, em parceria com seu eixo do 'bem': a reinserção da espionagem na agenda das relações internacionais a partir do caso Snowden é, em tese, o ápice de um processo de alteração de paradigmas no sistema internacional que vem se acentuando desde o fim da Guerra Fria e da queda das torres gêmeas em 11 de setembro de 2001, eventos decisivos para a securitização do 'terrorismo' por parte dos EUA, que logram associar o combate a esse inimigo 'sem face' a um largo sistema de vigilância global em que se confundem temáticas realmente essenciais à segurança nacional norte-americana com outras de cunho econômico, industrial ou meramente egoístas, que ferem a soberania dos países vigiados. O programa SILVERZEPHYR (figura 11) demonstra o foco de atenção que a América Latina tem tido nas preocupações dos EUA. Os principais alvos da operação de espionagem SILVERZEPHYR (nome de uma antiga linha de trem dos EUA) foram países da América Latina, que tiveram telefonemas, faxes e *e-mails* rastreados pelo software FAIRVIEW.

Figura 11 – Alvos do programa SILVERZEPHYR

Fonte: Jornal *O Globo* (http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/)

Observa-se, de cima para baixo e da esquerda para a direita: "US-3273 SILVERZEPHYR / Ponto de acesso à rede através de parceiro STEELKNIGHT. Opera sob a autoridade de trânsito / **Alvos-chave: Sul, Central e América Latina** / (Autoridade de Trânsito) - Metadados, Voz, Fax / (Coleção FAA) - Conteúdo e Metadados (*tradução livre, grifo nosso*).

Os processos de integração latino-americanos e caribenhos, na percepção dos EUA, geram preocupação, porque sugerem o início de um processo de autonomia regional que pode vir a desestabilizar sua tradicional 'zona de influência'. Nesse sentido, a indistinção dos países monitorados eleva a espionagem a um problema de segurança comum e regional. No caso sul-americano, reforça a parte sul da América como 'um conjunto de unidades cujos principais processos de securitização, dessecuritização, ou ambos, são tão interligados que seus problemas de segurança não podem ser razoavelmente analisados ou resolvidos separados uns dos outros' (Buzan & Waever, 2003). Dessa maneira, o enfrentamento de um problema comum, por essa lógica, deve se dar de forma conjunta e integrada.

Sem prejuízos das demais instâncias já integradas ou também em processo de integração (na verdade, reforçado por elas), e uma vez que a tentativa de suprir o descompasso tecnológico só se vislumbra a longo prazo, entendemos ser a integração dos serviços de inteligência, nos moldes de uma diplomacia de defesa,[25] a maneira mais estratégica de tornar efetivos os serviços de contra-inteligência sul-americanos. Por isso seria necessário, por exemplo, conhecer verticalmente o setor de inteligência de cada um dos países-membros da UNASUL e analisar o grau atual de integração entre eles, visando a catapultar uma integração completa, ou, pelo menos, uma cooperação de resultados na América do Sul, especialmente por que um dos métodos mais tradicionais de abordagem e atuação dos EUA, estendido agora às empresas de comunicação, é a cooptação de agentes de serviços de inteligência inimigos e a 'cooperação relativa' com os amigos, como ocorre nos 'cinco olhos'.

[25] Nos termos postos por Antônio Ruy de Almeida Silva (2013 - Defesa da Amazônia: VII ENABED): *Conjunto de práticas sociais específicas de agentes oficiais, constituídas no tempo e no espaço, para a administração das relações não coercitivas no âmbito da Defesa entre os Estados e outras entidades que atuam na política mundial.*

3. CONSIDERAÇÕES FINAIS

Iniciamos esta reflexão introduzindo a definição de inteligência e distinguindo-a do conceito de espionagem, que passamos a considerar como uma forma ilegal de obtenção de informações. Discorremos sobre as origens e o desenvolvimento da espionagem ao longo da história, procurando mostrar a antiguidade da prática e, por isso mesmo, qual teria sido a grande novidade trazida com os arquivos Snowden. Contextualizamos nosso marco teórico (os Estudos de Segurança Internacional e a Escola de Copenhague) e estruturamos a divisão de nosso trabalho seguindo as forças motrizes propostas por Buzan: política das grandes potências, eventos, tecnologia, debates acadêmicos e institucionalização, além de termos incluído um subitem específico (soberania). Na primeira, apresentamos um panorama da história dos EUA, chamando a atenção para a sobreposição entre serviços de inteligência (e/ou espionagem) e as decisões estatais. Na segunda, oferecemos um painel sobre os principais eventos históricos influenciadores da temática estudada, destacando o fim da Guerra Fria, a queda das torres gêmeas, a batalha de Seatle, a criação do WikiLeaks, o contencioso da informática entre Brasil x EUA e a privatização das telecomunicações brasileiras. Na terceira, traçamos uma linha temporal resgatando as revoluções técnicas e destacando as principais inovações no âmbito da espionagem (radar, criptografia, rádio, fotografia, microeletrônica e internet, por exemplo). Na quarta, incluímos no mesmo subcapítulo os debates acadêmicos e a institucionalização, crendo ser ainda insipiente a existência de teorias brasileiras sobre espionagem debatidas nas universidades, o que refreia a institucionalidade e os financiamentos para a temática. Na quinta, fizemos uma exposição lacônica dos principais pontos que julgamos necessários para a compreensão da imbricação entre as espionagens e a soberania, defendendo e provando que houve violação da soberania brasileira pelos EUA.

A conclusão a que se chega com este trabalho é a de que, antes de tudo, a materialização da prática de espionar pelos EUA só pôde ocorrer graças a uma condição específica que este país ocupou e ocupa no sistema internacional. Tal condição foi conquistada ao longo de uma história marcada por um processo veloz de industrialização, expansão territorial e imperialismo, cuja consolidação foi se dando assessorada pelos serviços de inteligência, que não raramente extrapolaram suas funções de suprir o Estado com apenas relatórios e informações processadas. Enredados em um sistema capitalista cuja forma de produção exploratória valoriza o individualismo e a lucratividade, os EUA alimentaram e foram alimentados por uma lógica de constante maximização de seus múltiplos poderes, envolvendo-se e sendo envolvidos por

eventos dos quais saíram cada vez mais poderosos e cujo ápice foi o fim da Guerra Fria. Com o excedente obtido durante a Segunda Revolução Industrial, foram capazes de financiar a Revolução Tecnológica e adentrarem no século XXI dominando física e metafisicamente todas as etapas da produção tecnológica baseada na microeletrônica, o que, na sequência, garantir-lhes-ia, além do domínio das infraestruturas, o completo controle do espaço virtual da sociedade em rede, posto, entre outras razões, terem sido seu precursor (Arpanet). Um evento específico, no entanto, em setembro de 2001, foi capaz de relativizar sua hegemonia e provocar uma preocupação ainda não experimentada: a de sofrer graves baixas no próprio território. A partir de então, encrudesceram a prática da espionagem e, em nome de um inimigo invisível, auto atribuíram o direito de ter todos os direitos. Sob essa condição e detendo os meios para fazê-lo, fizeram-no. A ação unilateral, porém, uma vez revelada, expôs a contradição entre a pregação e o pregador: em nome da soberania defendida para si acabaram violando a soberania alheia, constituindo este o maior dilema entre espionagem e soberania. Aos espionados, alguns mais outros menos, restou reconhecer a inferioridade tecnológica e, na sequência, tentar diminuí-la e/ou buscar reconfigurações de alianças de forma a tornar menos vulneráveis seus dados sensíveis.

Em relação ao Brasil, igualmente como a história explica a condição norte-americana, também o faz no caso brasileiro: inserido no sistema internacional em um momento de expansão do capitalismo, o Brasil se efetiva como fornecedor de matérias-primas e ao longo de anos vê sua dependência reforçada pela deterioração dos termos de troca, amenizada com o processo de substituição de importações e a consequente industrialização no século XX, o que lhe permite entrar no século XXI menos vulnerável, mas, no caso do setor de informática, igualmente dependente, por conta, na década de 1980, do contencioso com os mesmos EUA, que acabaram inviabilizando uma indústria nacional de informática, e, nos anos 1990, por conta da privatização das telecomunicações, que acaba, conforme o caso Snowden mostrou, por favorecer acordos entre o setor empresarial transnacional de telecomunicações do Brasil e o sistema de espionagem dos EUA.

Conclui-se também que, não obstante ter tido um sistema de informações originalmente voltado para o combate a inimigos internos e fortemente alinhado ao departamento de estado norte-americano, o Brasil, em 1999, concebeu sua própria agência de inteligência, entretanto fortemente marcada pela burocracia e pela exagerada cautela na determinação de ameaças vindas do interior. Essas características combinadas insinuam a fragilidade da Abin em ter se antecipado aos monitoramentos estadunidenses, fragilidade essa relativizada, diante, por exemplo, da igualmente incapacidade alemã em descobrir a mesma vigilância diante de seus

olhos. O caso Snowden também nos levou à conclusão de que, como consequência da flutuação dos próprios serviços de inteligência, os debates acadêmicos e a institucionalização da temática no Brasil são modestos, dificultando a geração de um corpo crítico capaz de provocar um ciclo criativo entre a prática e a reflexão sobre os serviços de inteligência, agravando a situação o fato de, sem massa crítica, ficarmos a mercê de ideias estranhas aos nossos interesses.

No que diz respeito à soberania, conclui-se, em termos estritamente da lei brasileira, que a interceptação das ligações telefônicas constituiu crime de violação da Lei 9.296/96, sem contar os danos indiretos que poderiam – ou podem – advir do conhecimento por terceiros de informações de setores sensíveis do Estado brasileiro. Apesar disso, a constatação do ato criminoso de quebra de soberania, diante da anarquia do sistema internacional, mostra-se atraente e útil mais como recurso político para buscar soluções negociadas no âmbito da ONU (como a aprovação da resolução proposta por Brasil e Alemanha em setembro de 2013) ou de outros órgãos multilaterais, do que necessariamente um argumento válido diante dos EUA.

Em termos mais abrangentes, quatro conclusões devem ser destacadas. Uma é que o indivíduo foi alçado à condição de ator e agente do sistema internacional, sendo capaz de alterá-lo. Outra é que a espionagem foi reinserida na agenda internacional, provocando mobilizações nos mais diversos graus, desde reconsiderações de alianças e/ou criações de novas, passando pela discussão de uma governança para a internet e por debates sobre uma legislação internacional sobre crimes cibernéticos, até alterações na forma de enxergar como as infraestruturas estão distribuídas, especialmente no que diz respeito a cabos submarinos e a satélites de transmissão. A América do Sul, território latino-americano livre de armas nucleares, talvez devesse seriamente considerar, nesse quadro, a hipótese de buscar a integração dos seus serviços de inteligência, podendo, como parte do sistema de segurança e defesa sul-americano, tornar-se o principal elo entre os governos, as sociedades e os exércitos, conciliando os propósitos políticos dirigidos pelos chefes de Estado ou governo com os interesses sociais e o planejamento estratégico consoante a condução dos chefes militares ou forças armadas. A terceira é a de que se, por um lado, a sensação de ludíbrio causou desconfortos diplomáticos no Brasil e nos EUA, por outro, as revelações foram capazes de apontar qual percepção os EUA tinham – e têm – do Brasil, o que pode auxiliar o Estado brasileiro a reorganizar-se estrategicamente frente aos EUA, de acordo com as intenções que são possíveis de captar no interesse norte-americano em relação àquilo que especificamente espionaram no Brasil, um tipo de segredo jamais encontrado senão por meio de delações como a realizada por Snowden. Por último, é emergente que o Brasil mobilize sua diplomacia, associada aos recursos de inteligência do Estado, para torna-se um agente influente na agenda da governança da internet.

REFERÊNCIAS

AFONSO, Leonardo Singer (2006). ***Considerações sobre a relação entre a inteligência e seus usuários***. In: REVISTA BRASILEIRA DE INTELIGÊNCIA / Agência Brasileira de Inteligência. – n. 5(out. 2009) – Brasília, Abin.

ANDRÉ DE MELLO e Souza (Org.); NASSER, R. M**.** (Org.); MORAES, R. F. (Org.) (2014). ***Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século***. 1. ed. Brasília, Instituto de Pesquisa Econômica Aplicada Ipea.

BANDEIRA, Luiz Alberto Moniz (2010a). ***Geopolítica e política exterior – Estados Unidos, Brasil e América do Sul***. Brasília, FUNAG.

BANDEIRA, Luiz Alberto Moniz (2010b). ***Brasil, Argentina e Estados Unidos: conflito e integração na América do Sul (da Tríplice Aliança ao Mercosul), 1870-2007***. 3.ed., ver. e ampl. – Rio de Janeiro, Civilização Brasileira.

BRASIL. ***Estratégia Nacional de Defesa*** (2008). Brasília. Disponível em: <http://defesa.gov.br> .

BRASIL. ***Portaria no 666, de 4 de agosto de 2010*** (2010a). Disponível em: <http://sgex.eb.mil.br> .

BRASIL. ***Portaria no 667, de 4 de agosto de 2010*** (2010b). Disponível em: <http://sgex.eb.mil.br>.

BUZAN, Barry; HANSEN, Lene (2012). ***A evolução dos estudos de segurança internacional***. São Paulo, Ed. Unesp.

BUZAN, Barry (1998). ***Security: a new framework for analysis***. London, Lynne Rienner Publishers.

BUZAN, Barry (2003). **Regions and powers: the structure of international security**. Cambridge, Cambridge University Press.

CASTELLS, Manuel. **A Sociedade em Rede: do Conhecimento à Política**. *In*: CASTELLS, Manuel & CARDOSO. (2005). [org]. ***A Sociedade em Rede: Do Conhecimento à Acção Política***. Conferência promovida pelo Presidente da República de Portugal entre 4 e 5 de Março de 2005, no Centro Cultural de Belém. Imprensa Nacional: Casa da Moeda, 2005.

CAVALCANTE, Sávio. **As telecomunicações após uma década da privatização: a face oculta do "sucesso"** (Abr.2011)**.** *Revista de Economia Política das Tecnologias da Informação e da Comunicação*. Vol. XIII, n.1, Ene.

CEPIK, Marco A. C. (2001a) ***Serviços de Inteligência: Agilidade e Transparência como dilemas de institucionalização***. Tese de doutorado apresentada no IRPERJ.

CEPIK, Marco A. C. (2001b). **Segredos Públicos: um dilema democrático**. *Insight Inteligência – Voyeurismo*. Julho-Agosto-Setembro

CEPIK, Marco A.C. (2002/2003). **Inteligência e Políticas Públicas: dinâmicas operacionais e condições de legitimação**. *Security and Defense Studies Review*. Vol.2 Winter.

CEPIK, Marco A.C. (2005). **Regime político e sistemas de Inteligência no Brasil: legitimidade e efetividade como desafios institucionais**. *DADOS – Revista de Ciências Sociais*, Rio de Janeiro, Vol. 48, nº 1.

CEPIK, Marco A.C. (2014) **A securitização do ciberespaço e o terrorismo: uma abordagem crítica.** *In***:** ANDRÉ DE MELLO e Souza; NASSER, R. M.; MORAES, R. F. (2014) [orgs.]. ***Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século***. 1. ed. Brasília: Instituto de Pesquisa Econômica Aplicada Ipea, 2014, pp.. 161-186)

CERVO, Amado Luiz (2008). ***Inserção internacional: formação dos conceitos brasileiros***. São Paulo, Saraiva.

DUQUE, Maria Guedes (2009). **O papel de síntese da escola de Copenhague nos estudos de segurança internacional.** *Contexto Internacional*, vol.31, número 3, Rio de Janeiro Sept./Dec.

FIORI, Jose Luís (2007). ***O poder global e a nova geopolítica das nações***. São Paulo, Boitempo Editorial.

GREENWALD, Glenn (2014). ***Sem lugar para se esconder: Edward Snowden, a NSA e a espionagem do governo americano***. Tradução de Fernanda Abreu. Rio de Janeiro, Sextante.

HARDING, LUKE (2014). ***Os arquivos Snowden: a história secreta do homem mais procurado do mundo***. Tradução de Alice Klesck, Bruno Correia. Rio de Janeiro, LeYa.

HOBSBAWM, Eric J. (1996). ***A era do capital***. Rio de Janeiro, Paz e Terra.

HOBSBAWM, Eric J. (1998). ***A era dos impérios***. Tradução de Sieni Maria Campos e Yolanda Steidel de Toledo. Rio de Janeiro, Paz e Terra.

KARNAL, Leandro; PURDY, Sean; FERNANDES, Luiz Estevam; MORAIS, Marcus Vinícius de (2007). ***História dos Estados Unidos das origens ao século XXI***. São Paulo, Contexto.

KEEGAN, John (2006). ***Inteligência na guerra: conhecimento do inimigo, de Napoleão à Al-Qaeda***. Tradução de S. Duarte. Companhia das Letras, São Paulo, SP.

LUCAS KERR de Oliveira. **A Geopolítica Clássica e as Novas Geopolíticas: perspectivas para A Defesa da Amazônia, do Pré-Sal e da Integração Regional Sul-Americana**. *Seminário "Novas geopolíticas e a Pan-Amazônia"*, 09 de julho de 2013. Instituto Pandiá Calógeras e pelo Centro de Estudos Estratégicos do Exército, Ministério da Defesa. Brasília, DF.

LUCERO, Everton (2011). ***Governança da internet: aspectos da formação de um regime global e oportunidades para a ação diplomática***. Fundação Alexandre de Gusmão, Brasília, DF.

MATOS FILHO, José C. e OLIVEIRA, Carlos W. (1996) *O* ***Processo de Privatização das Empresas Brasileiras***. Brasília, IPEA.

PILLAS, Jean-Marc (1996). ***Nossos agentes em Havana***. Tradução Christina Cabo. – Rio de Janeiro, Record.

PIRES, Hindenburgo Francisco (2012). **Estados nacionais, soberania e regulação da Internet**. *Scripta Nova. Revista Electrónica de Geografía y Ciencias Sociales.* [En línea]. Barcelona: Universidad de Barcelona, 1 de noviembre de 2012, vol. XVI, nº 418 (63). <http://www.ub.es/geocrit/sn/sn-418/sn-418-63.htm>. [ISSN: 1138-9788]

REALE, Miguel (2000). ***Teoria do Direito e do Estado***. São Paulo, Saraiva.

SAHD, Fábio Bacila (2012). ***Sionismo, modernidade e barbárie: vida e morte na Faixa de Gaza***. Curitiba, Graciosa.

SANTOS, Milton (2008). ***A natureza do espaço: técnica e tempo, razão e emoção***. São Paulo, Editora da Universidade de São Paulo.

SISTEMA BRASILEIRO DE INTELIGÊNCIA. Conselho Consultivo (2004). ***Manual de Inteligência: Doutrina Nacional de Inteligência: bases comuns***. Brasília: Abin, 44 p.

VIGEVANI, Tullo (1995). ***O contencioso Brasil x Estados Unidos da informática: uma análise sobre a formulação da política exterior***. São Paulo: Alfa Omega, Editora da Universidade de São Paulo.

VIZENTINI, Paulo G. F. SADER, Emir (2004) [orgs.]. **O descompasso entre as nações**. Record: Rio de Janeiro.

VOLKMAN, Ernest (2013). ***A história da espionagem: o mundo clandestino da vigilância, espionagem e inteligência, desde os tempos antigos até o mundo pós-9/11***. Título Original: The History of Espionage. Editora Escala Ltda, São Paulo.